The Sedona Conference Journal®

Volume 17 ❖ 2016 ❖ Number One

Articles

The Sedona Conference®

Antitrust Law, Complex Litigation, and Intellectual Property Rights

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual or semi-annual basis, containing selections from the preceding year's conferences and Working Group efforts. The Journal is available on a complimentary basis to courthouses and public law libraries and by annual subscription to others ($95; $45 for conference participants and Working Group members). Send us an email (info@sedonaconference.org) or call (1-602-258-4910) to order or for further information. Check our website for further information about our conferences, Working Groups, and publications: www.thesedonaconference.org.

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:
The Sedona Conference, 301 East Bethany Home Road, Suite C-297, Phoenix, AZ 85012 or info@sedonaconference.org or call 1-602-258-4910.

The Sedona Conference Journal® designed by MargoBDesignLLC at www.margobdesign.com or mbraman@sedona.net.

Cite items in this volume to "17 Sedona Conf. J. _____ (2016)."

Copyright 2016, The Sedona Conference.
All Rights Reserved.

THE SEDONA CANADA PRINCIPLES ADDRESSING ELECTRONIC DISCOVERY, SECOND EDITION*

A Project of The Sedona Conference Working Group on Sedona Canada (WG7)

Author: The Sedona Conference

Editor-in-Chief: Susan Nickle

Managing Editor: Jim W. Ko

Contributing Editors:

Anne Glover
Crystal O'Donnell
David N. Sharpe

Contributors:

Hon. Colin L. Campbell Q.C.
Roger B. Campbell
Robert J.C. Deane
Karen B. Groulx
David Outerbridge
James T. Swanson
Susan Wortzman

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 7. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any organizations to which they may belong, nor do they necessarily represent official positions of The Sedona Conference.

---

* Copyright 2015, The Sedona Conference. All Rights Reserved. "Sedona Canada" is a registered trademark in the Canadian Intellectual Property Office.

We thank all of our Working Group Series Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, click on the "Sponsors" navigation bar on the homepage of our website.

*****

Editorial and Steering Committees (2008 ed.):

Hon. Colin L. Campbell Q.C.
Robert J.C. Deane
Peg Duncan
David Gray
Dominic Jaar (Editor, French Language Edition)
Justice J.E. Scanlan
Glenn Smith
Susan Wortzman
John H. Jessen, Technology Advisor

PREFACE

Welcome to the Second Edition of *The Sedona Canada Principles Addressing Electronic Discovery*, a project of The Sedona Conference Working Group on E-Discovery Issues in Canada ("Sedona Canada" or "WG7"). This is one of a series of working group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute that exists to allow leading jurists, lawyers, experts, academics, and others, at the cutting edge of issues in the areas of antitrust law, complex litigation, and intellectual property rights, in conferences and mini-think tanks called Working Groups, to engage in true dialogue, not debate, in an effort to move the law forward in a reasoned and just way.

WG7 was formed in 2006 with the mission "to create forward-looking principles and best practice recommendations for lawyers, courts, businesses, and others who regularly confront e-discovery issues in Canada." The first edition of these *Sedona Canada Principles* was released in early 2008 (in both English and French) and was immediately recognized by federal and provincial courts as an authoritative source of guidance for Canadian practitioners. It was explicitly referenced in the Ontario *Rules of Civil Procedure* and practice directives that went into effect in January 2010.

The Second Edition represents the collective efforts of many individual contributors. The drafting process for the Second Edition was initiated in October 2012 by a large group of Canadian practitioners, and was both developed and brought to consensus by the drafting team over an extensive process including countless conference calls. The draft was also the focus of dialogue at The Sedona Conference WG7 Meeting in Toronto, in August 2014. The Public Comment Version of the Second Edition was published in February 2015, and the editors have reviewed the comments received through the public comment process.

On behalf of The Sedona Conference, I thank all drafting team members for their time and attention during the drafting and editing process, including Susan Nickle, Anne Glover, Crystal O'Donnell, Da-

vid N. Sharpe, Hon. Colin L. Campbell Q.C., Roger B. Campbell, Robert J.C. Deane, Karen B. Groulx, David Outerbridge, James Swanson, and Susan Wortzman. I also thank volunteer Nadia Sayed. I further thank Luc Bélanger, Justice David M. Brown, Ronald Davis, Martin Felsky, Kelly Friedman, Heidi Lazar-Meyn, Kathryn Manning, Lynne Vicars, and, in particular, William E. Hoffman, and everyone else involved in this extensive project, for their assistance and contributions to this effort.

I also thank the original WG7 Editorial and Steering Committee members who brought to publication the First Edition of the *Sedona Canada Principles* in January 2008, including Hon. Colon L. Campbell Q.C., Robert J.C. Deane, Peg Duncan, David Gray, Dominic Jaar, Justice J.E. Scanlan, Glenn Smith, and Susan Wortzman, as well as the Technology Advisor, John H. Jessen.

Working Group Series output is first published in draft form and widely distributed for review, critique, and comment, including in-depth analysis at Sedona-sponsored conferences. Following this period of peer review, the draft publication is reviewed and revised by the Working Group and members of the Working Group Steering Committee, taking into consideration what is learned during the public comment period. Please send comments to info@sedonaconference.org, or fax them to 602-258-2499. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be.

Craig W. Weinlein
Executive Director
The Sedona Conference
November 2015

FOREWORD

The *Sedona Canada Principles* (the "*Principles*") were originally published in January 2008.[1] Since that time, the Canadian electronic discovery ("e-discovery") environment has matured significantly.

In 2008, the writers of the *Principles* necessarily advocated for cultural change in the legal profession to address the impact of e-discovery on the litigation process. Over the past seven years, we have seen notable changes: rules have been amended to accommodate e-discovery, a robust body of Canadian e-discovery case law has developed, the test for relevance has been narrowed in some jurisdictions to reflect a new, high volume, "e-reality," and across the country, the concept of proportionality has become firmly entrenched in the new discovery vernacular.

Now in 2015, further changes in legal culture are still required. Central to this shift is early and meaningful cooperation between counsel, as well as the acknowledgement that basic e-discovery principles apply to cases of every size and subject matter. The amended *Principles* presented below reflect these important ideals, as well as other important developments in Canadian law. In an effort to make the *Principles* as accessible to

1. The *Sedona Canada Principles* are the work of The Sedona Canada Working Group, which is Working Group 7 (WG7 or the "Working Group") of the Sedona Conference. The Sedona Conference was formed in 1997 in Sedona, Arizona, and is currently based in Phoenix, Arizona. The Sedona Conference, its *Principles* and its numerous publications and initiatives have been instrumental throughout the world in the development and promulgation of standards and best practices in the use of electronic information in litigation and other forms of investigation.

as wide an audience as possible, the Working Group has distilled the following updated *Principles* and associated Commentary into the following core statements:

The *Sedona Canada Principles* are focused on the discovery process. Issues related to the management of electronic records and other electronically stored information (ESI) are increasingly important from a business and legal point of view. Under the various Evidence Acts in Canada, the admissibility of electronic records as evidence often requires having regard to the integrity of the operation and functions of information systems and of the records they house and manage. There are current and emerging standards related to electronic records management systems and policies which are helpful and valuable in the general management of the life cycle of ESI, including authenticating and proving electronic records as evidence. However, records and information governance policies and practices, the integrity and operation of information systems and software, and the substantive law related to the admissibility of electronic records are in large part all beyond the scope of these *Principles*. Instead, the *Principles* focus on best practices related to the discovery process in the circumstances in which parties to litigation find themselves, and not the ways parties could have managed their systems and records before litigation arises, in order to improve their ability to deal with litigation and discovery obligations.

The *Sedona Canada Principles* are at the centre of the discovery process in Canada. The *Principles* provide an outline of best practices with respect to the management of ESI that are or may be relevant to every case. First published in January 2008, they have been the basis of formal rule amendments in at least two Provinces. They provide for the cooperative management of the discovery phase, which, due to the proliferation of

ESI, has an increasingly central role in the conduct of a civil action.

The *Sedona Canada Principles* provide practical guidelines. The *Principles* are flexible enough that practitioners and judges can use them when dealing with ESI in different case types; when assessing the effects of different sources, formats and volumes of ESI; and when determining the relative costs and benefits of adopting different forms of documentary production.

ESI is ubiquitous. Lawyers at all levels should be comfortable with managing ESI. Electronic communication now reaches into almost all aspects of our lives. The vast majority of information produced in the world today is electronic and will never be printed. ESI is present in virtually every case, meaning that all lawyers must have a basic knowledge of how to manage it.

Parties have an obligation to preserve potentially relevant ESI in the context of litigation, regulatory matters and audits. The duty to preserve potentially relevant information, when triggered, extends to ESI.

ESI behaves completely differently than paper documents. There are thousands of electronic file formats. Computer systems now replicate and distribute ESI without active human involvement. Duplicates and near-duplicates proliferate on the user's computer and elsewhere. As systems change, ESI can become less accessible and therefore harder to preserve and collect. The methods of searching, retrieving, converting and producing ESI are completely different from those relating to paper and are constantly evolving.

1. ESI can be mishandled in ways that are unknown in the world of paper. Electronic information can be overwritten, hidden, altered and even completely deleted

through inadvertent, incompetent, negligent or illicit handling without these effects being known until later. It is therefore important to identify potentially relevant ESI and to preserve it as soon as possible in a manner that protects the integrity of the information. Understanding the basics of how ESI should be handled will help to minimize these risks while providing counsel with the knowledge to hold other parties to account. Counsel have a professional responsibility to advise clients of appropriate practices and the risks of not employing them.

2. Preservation of ESI is crucial. The special characteristics of ESI and the constant evolution of technology mean that it is critical, when meeting discovery obligations, to take prompt and active measures to preserve potentially relevant ESI in a defensible manner that protects the integrity of the information.
3. Large organizations and individual parties can equally threaten the loss of relevant ESI. Each entity or person may handle ESI differently and each can lose or alter potentially relevant ESI unless steps are taken to preserve it. Corporations may purge some ESI every day, but they have backup systems. Individuals may only purge ESI less frequently; but, when they do, it may likely be lost forever.
4. ESI raises special challenges with respect to authentication. Only proper methods for preserving, collecting, processing, reviewing and producing ESI will defensibly protect data integrity and maintain chain of custody. Copying and moving ESI without using proper methods will almost always change some of its metadata.

For all the above reasons, it is important for counsel to learn about efficient and defensible methods for handling ESI—

whether with respect to initial preservation, subsequent collection, processing, review or production.

ESI can be relevant in even the smallest cases. ESI is not confined to large, complex or high-profile cases. It is relevant in almost every civil litigation matter, including personal injury and family law litigation. It can be important even in very small or simple cases—for example, where the case turns on the information contained on a cell phone or in e-mail.

Small cases may give rise to their own procedures and expectations. Rules and practices that make sense for large entities may not make sense for individual litigants. A large corporation would be expected to have a document retention policy; an individual would not. To expect a large multinational corporation to put a hold on all its physical computer devices would be disproportionate in almost all cases; to expect an individual plaintiff to preserve his or her cell phone and all its social media content may not be.

All e-discovery should be conducted with a view to what is proportionate in the circumstances. Proportionality is the barometer applied to the question of how much time, effort and expense a party should reasonably have to expend with respect to ESI in light of all relevant factors. Every jurisdiction that has adopted ESI-related rules of procedure that impose affirmative obligations has adopted a proportionality principle. All ESI is potentially discoverable and parties have a duty to preserve, search and then produce what meets the relevant test for disclosure. But no party is required to preserve, search and produce all (or particularly problematic sets of) ESI where to do so would impose costs and burdens disproportionate to the value of the case or the probative value of the evidence in question, taking into account the availability of the same information from other sources and other factors. (*See* Principle 2).

Core principles and best practices apply everywhere, regardless of the size of the case. Early discussions between opposing counsel and cooperation regarding the management of all aspects of ESI are important in all cases. Even if the scope, volume and methods differ, the key elements of cooperation and the development of a discovery plan remain the same: what is at issue, who are the key individuals, what are the sources of information, what should be preserved, in what order should information be collected and processed, in what formats will the parties review and produce, and so on. Of these types of issues, search methods can be the most important. In smaller cases there may be no access to sophisticated tools. In such cases, the proper handling of ESI may be of *greater* immediate concern than it is in larger cases.

Parties should confer as early as possible to work out reasonable ways of meeting their discovery obligations. The *Principles* call for meaningful and ongoing cooperation between parties throughout discovery. Parties are called upon: to confer as soon as practicable and on an ongoing basis to facilitate cooperative resolution of all discovery issues (*see* Principle 4); to agree as early as possible on production formats and the contents of various listings (*see* Principle 8); and to agree or seek direction on how to protect privileges, privacy, trade secrets and other confidential information (*see* Principle 9).

Ongoing cooperation and conferring between parties can minimize burdens, mitigate risks and lead to the speedier resolution of disputes. By engaging in early and ongoing discussions regarding the identification, preservation, collection, processing, review and production phases, and by sharing, as appropriate, information about relevant subsets of ESI (data preserved, data collected, search results, etc.), parties can gain tremendous efficiencies by reducing, at the outset, and thereafter at each subsequent stage, the volume of information they

have to collect, process, search, review and produce. This approach can replace the traditional practice whereby each party prepares a listing of relevant documents, and in some cases may even proceed to produce the entirety of what it believes to be relevant documents, without consultation with the other parties.

Early, ongoing and meaningful cooperation between the parties can minimize costs, reduce delay, avoid the kinds of mistakes and confusion that arise from failures to communicate and avoid costly and time-consuming motions to deal with otherwise manageable discovery disputes.

Lawyers should accept document production in electronic form and understand the e-discovery components in each of their cases. The most important evidence in a case might be electronic; indeed, when the vast majority of communications are never printed, it almost certainly will be.

Managing information electronically allows for highly efficient organization, searching, review, analysis and production—far faster than what is possible with paper or scanned documents. It is faster, more efficient and cheaper to exchange electronic information and documents in electronic form than printing the electronic documents to paper and then reconverting the paper printouts to electronic form. This is true even in small cases. Modern tools allow for efficient collaborative discovery whereby all parties have access to relevant information, at lower cost per party, while enjoying all the benefits of electronic management and while maintaining all necessary partitions between datasets. Further, lawyers who avoid best practices for dealing with ESI may expose themselves to professional liability.

This Second Edition of the *Principles* continues to aim to assist in the resolution of what can be difficult and complex discovery disputes and, thus, to assist in reaching effective, timely, cost-efficient and defensible solutions to problems of document disclosure.

*****

The Sedona Canada Working Group has revised the original 2008 version of the *Principles* in a number of key areas. In several cases, the language of the Principles themselves has been modified. The Commentary under each of the Principles has been comprehensively updated, along with applicable case law where appropriate. The most significant amendments are summarized below as follows:

Principle 1

The Commentary for Principle 1 has been amended to add a reference to social media.

Principle 2

Principle 2 has been modified to create a five-part test for proportionality.

A new opening Commentary paragraph emphasizes the importance of the proportionality principle. A section dealing with the applicability of the proportionality principle to procedure and procedural motions has also been included.

The Commentary also now includes a reference to the E-Discovery Implementation Committee (EIC) of the Ontario Bar Association and its development of model documents.

Principle 3

The Commentary has been amended to emphasize the value and importance of information governance as a way of preparing for litigation and, in particular, for e-discovery.

Principle 4

Principle 4 has been amended to emphasize the concept of "cooperation" (versus "meet-and-confer") in developing a joint discovery plan.

There are important new sections and an overall shift in emphasis throughout the Commentary for this Principle. First, there is new emphasis on the importance and value of discovery planning. This section proposes that the term "meet-and-confer" be replaced with "discovery planning," "consultation" or any similar term that does not suggest that in-person meetings are required. Emphasis is placed on the good-faith sharing of information aimed at reaching agreement on a discovery plan.

Principle 5

The Commentary discussion in this Principle on data being "not reasonably accessible" and therefore being excluded from the set of ESI that needs to be dealt with has been removed. The fact that information has been deleted does not, on its own, mean that the data is not accessible or that a party has no obligation to obtain it.

Principle 6

Principle 6 now makes clear that "[a] party should not be required, absent agreement or a court order based on demonstrated need and relevance, to search for or collect deleted or residual ESI that has been deleted in the ordinary course of business or within the framework of a reasonable information governance structure." While a party may not simply delete information to thwart discovery obligations, defensible information governance principles will be considered.

The Commentary has been updated to include new Canadian case law supporting the proposition that the deletion of

documents is permissible in the normal course of business or pursuant to a reasonable document retention policy.

Principle 7

Principle 7 has been amended to clarify that this Principle applies not only to electronic records, but to records in any format.

In the Commentary, given the advancements in technology and the pace at which technology is developing and changing, references to any specific techniques or tools have been removed. Further, the discussion on tools that can be used by a party to satisfy its document discovery obligations has been expanded.

Lastly, a section on the importance of sampling and validating any method adopted to fulfill a party's discovery obligations has been added.

Principle 8

Principle 8 has been amended to remove the reference to "lists of documents" given the fact that many parties no longer exchange lists of documents. The proposed new Principle is simplified to read as follows: "Parties should agree as early as possible in the litigation process on the format, content and organization of information to be exchanged between the parties."

Additional information has been included in the section on "Agreeing on a Format for Production" given the change in the practice over the years to productions being made in native format where possible.

The section on "Document Lists – Format and Organization" has been renamed "Affidavits and the Format and Organization of Record Lists." This section has also been expanded to discuss the fact that the manual coding of documents is often no

longer required given the movement to producing native files (and collecting native files from clients).[2] A comment has also been included on the issues that have arisen in this new electronic age with the wording in certain Affidavits of Documents required by the applicable rules of court in certain provinces.

Principle 9

In the Commentary, there has been an expansion of the discussion on privilege and inadvertent disclosure. Further, a new section regarding the information on coded documents in a document list has been added.

A number of new sections regarding privacy in different contexts have been added, including privacy and social media, employee privacy on employer-issued devices and criminal investigations.

Lastly, a brief section on data security and chain-of-custody issues has been added.

Principle 10

The Principle has been changed to reflect different geographic jurisdictions and forums.

The Commentary has been substantially expanded to address areas of difference in cross-border litigation that counsel should consider, and it includes a brief discussion of issues that arise in cross-forum litigation, such as criminal and regulatory proceedings.

A section on the use of electronic evidence in arbitrations has also been added.

---

2. For a discussion of coding, see *infra*, Introduction, section F.8 (Advanced Technology Can Help to Organize, Search and Make Sense of ESI) and note 27.

Principle 11

The Principle has been amended to confirm that sanctions may be considered for a party's failure to meet any obligation with respect to any phase of discovery. A previous reference to a defaulting party avoiding sanctions if it demonstrates the failure was not intentional or reckless has been removed.

The Commentary describing the American experience has been removed and replaced with a discussion of the growing body of Canadian case law regarding spoliation and sanctions for nondisclosure.

The previous Commentary section on reasonable records management has been renamed and expanded to more broadly discuss information governance principles and rebutting the presumption of spoliation.

Principle 12

The Principle has been amended to confirm that the party producing ESI will generally bear its own costs of all phases of discovery.

The case law in the Commentary has been updated and a direct reference to proper information governance as a significant factor in reducing costs associated with e-discovery has been included.

Susan Nickle
Editor-in-Chief

Anne Glover
Crystal O'Donnell
David N. Sharpe
Contributing Editors

Hon. Colin L. Campbell Q.C.
James Swanson
Co-Chairs, Working Group 7 Steering Committee

TABLE OF CONTENTS

THE SEDONA CANADA PRINCIPLES ADDRESSING ELECTRONIC DISCOVERY—AT A GLANCE

Principle 1. Electronically stored information is discoverable.

Principle 2. In any proceeding, the parties should ensure that steps taken in the discovery process are proportionate, taking into account: (i) the nature and scope of the litigation; (ii) the importance and complexity of the issues and interests at stake and the amounts in controversy; (iii) the relevance of the available electronically stored information; (iv) the importance of the electronically stored information to the Court's adjudication in a given case; and (v) the costs, burden and delay that the discovery of the electronically stored information may impose on the parties.

Principle 3. As soon as litigation is reasonably anticipated, the parties must consider their obligation to take reasonable and good-faith steps to preserve potentially relevant electronically stored information.

Principle 4. Counsel and parties should cooperate in developing a joint discovery plan to address all aspects of discovery and should continue to cooperate throughout the discovery process, including the identification, preservation, collection, processing, review and production of electronically stored information.

Principle 5. The parties should be prepared to produce relevant electronically stored information that is

reasonably accessible in terms of cost and burden.

Principle 6. A party should not be required, absent agreement or a court order based on demonstrated need and relevance, to search for or collect deleted or residual electronically stored information that has been deleted in the ordinary course of business or within the framework of a reasonable information governance structure.

Principle 7. A party may use electronic tools and processes to satisfy its documentary discovery obligations.

Principle 8. The parties should agree as early as possible in the litigation process on the format, content and organization of information to be exchanged.

Principle 9. During the discovery process, the parties should agree to or seek judicial direction as necessary on measures to protect privileges, privacy, trade secrets and other confidential information relating to the production of electronically stored information.

Principle 10. During the discovery process, the parties should anticipate and respect the rules of the forum or jurisdiction in which the litigation takes place, while appreciating the impact any decisions may have in related proceedings in other forums or jurisdictions.

Principle 11. Sanctions should be considered by the Court where a party will be materially prejudiced by

another party's failure to meet its discovery obligations with respect to electronically stored information.

Principle 12. The reasonable costs of all phases of discovery of electronically stored information should generally be borne by the party producing it. In limited circumstances, it may be appropriate for the parties to arrive at a different allocation of costs on an interim basis, by either agreement or court order.

I. INTRODUCTION TO THE SECOND EDITION: DISCOVERY IN TODAY'S WORLD OF ELECTRONICALLY STORED INFORMATION

The rapid transformation of information and technology continues to present challenges to the legal profession. In the first decade of this century, the courts and the legal profession began to meet this challenge in earnest. A few milestones of note:

1. Following the release in the United States of the first public comment draft of *The Sedona Principles* in 2003, a set of changes in late 2006 to the U.S. Federal Rules of Civil Procedure relating to electronically stored information (ESI)[3] and several well-publicized U.S. federal court decisions, the Sedona Canada Working Group 7 (WG7 or the "Working Group") was formed in 2006.
2. The first edition of these *Sedona Canada Principles Addressing Electronic Discovery* (the "*Sedona Canada Principles*" or the "*Principles*") was released in January 2008.[4]
3. Nova Scotia became the first Canadian province to amend its *Rules of Civil Procedure* to address electronic discovery by the insertion of a new Rule 16[5] in 2008; these amendments were based on the *Principles*.[6]

---

3. Federal Rules of Civil Procedure: Title V. Disclosure and Discovery: Rule 26 at "Committee Notes on Rules - 2006 Amendment," online: Legal Information Institute <http://www.law.cornell.edu/rules/frcp/rule_26>.

4. The Sedona Conference, *The Sedona Canada Principles Addressing Electronic Discovery* (January 2008), online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/71>.

5. *Nova Scotia Civil Procedure Rules*, Royal Gazette Nov 19, 2008, at r 16.

6. Nova Scotia Barristers' Society, Table of Concordance: (from CPR 2008 to CPR 1972) at 4, online: Nova Scotia Barristers' Society <http://nslaw.nsbs.org/nslaw/concordance.do>.

4. On January 1, 2010, Ontario amended its *Rules of Civil Procedure* to include two new rules: Rule 29.1 (Discovery Plan) and Rule 29.2. (Proportionality in Discovery).[7] Rule 29.1 imposes an affirmative obligation on the parties to agree to a discovery plan and requires that "[i]n preparing the discovery plan, the parties shall consult and have regard to the document titled *The Sedona Canada Principles Addressing Electronic Discovery* developed by and available from The Sedona Conference®."
5. On September 5, 2014, the Ontario Superior Court of Justice released its decision in *Palmerston Grain v. Royal Bank of Canada*.[8] In a strongly worded decision, the Court held that parties are required to comply with the *Sedona Canada Principles* and failing to do so is a breach of the *Rules of Civil Procedure*, effectively making the Principles mandatory for Ontario cases dealing with electronic information.

As the *Sedona Canada Principles* have come to play a prominent role in Canadian civil procedure, it is important to remember that they are not a set of national rules; they are a set of guidelines and best practices that can assist parties and judges in deciding how best to manage ESI during discovery, in a range of circumstances.

A. What is Electronic Discovery?

Electronic discovery ("e-discovery") refers to the discovery of ESI. Information is "electronic" if it exists in a medium that can be, or needs to be, read using computers or other digital

7. The enacting regulation affecting this amendment was O Reg. 438/08, ss. 25–26.

8. [2014] O.J. No. 4132.

devices. Electronic media include magnetic disks, optical disks, magnetic tape and solid state drives. Electronic information can come in the form of e-mails, word-processing files, spreadsheets, web pages, databases, video recordings, sound recordings and thousands of other formats.

Electronic discovery differs from traditional paper discovery in a number of ways, which are discussed in more detail below. One fundamental difference is that electronic data requires the use of electronic devices and software and, therefore, the direct or indirect support and involvement of software developers, computer technicians and other specialists.

B. To Whom are these *Principles* Addressed?

These *Principles* and their associated Commentary are addressed to anyone who works with electronic evidence for legal or other investigative purposes. At a minimum, all such people need to understand certain basic technical facts regarding how ESI is created, stored, manipulated and used for evidentiary purposes.[9] They also must be familiar with the guidance, recommendations and best practices provided in these *Principles*. It is now impossible to understand the scope of, and to perform one's obligations concerning, the handling of evidence without extending those obligations and understanding to electronic information.

The Working Group continues to encourage a broader understanding and acceptance of these *Principles* in the Canadian legal and investigative community. It is not merely litiga-

9. For a convenient reference to technical terms relevant to electronic discovery, see The Sedona Conference, *Glossary For E-Discovery and Digital Information Management* (April 2014), online: The Sedona Conference <https://thesedonaconference.org/download-pub/3757>.

tors involved in large cases who should develop their understanding in this area. All persons involved in the legal community will benefit from greater familiarity with and adoption of these *Principles*.

C. What Rules Govern Electronic Document Production in Canada?

In Canada, the rules for documentary production are governed by each province's rules of civil procedure or rules of court. Each court in Canada, whether provincially or federally instituted, has a rule requiring the production of documents relevant to matters in issue in the action, along with a definition of "document" that includes electronic records or data. Each province, territory and federal jurisdiction has a well-developed set of rules regulating the production, inspection, and listing of

documents that are relevant to the proceedings at hand.[10] [11] While the approach varies from jurisdiction to jurisdiction, the Rules of most Provinces and Territories are similar.

D. Why Do Courts and Litigants Need Standards Tailored to Electronic Discovery?

Prior to the first publication of these *Principles* in 2008 it could be said that e-discovery was uncommon. Most counsel were unfamiliar with ESI and its special requirements. In most jurisdictions, neither the courts nor other litigating parties had

---

10. The general rules requiring documentary production are found at the following sections in the relevant province's rules: Ontario *Rules of Civil Procedure,* RRO 1990, O Reg 194, r 30.02 [*Ontario Rules*]; Alberta *Rules of Court*, Alta Reg 124/2010, Part 5 [*Alberta Rules*]; British Columbia *Supreme Court Civil Rules*, BC Reg 168/2009, r 7-1 [*BC Rules*]; Manitoba *Court of Queen's Bench Rules*, Man Reg 553/88, r 30.02 [*Manitoba Rules*]; New Brunswick *Rules of Court*, NB Reg 82-73, r 31.02 [*NB Rules]*; Newfoundland and Labrador *Rules of the Supreme Court*, SNL 1986 c 42, Sch. D, r 32.01 and 32.04; Northwest Territories *Rules of the Supreme Court*, NWT Reg 010-96, r 219, 225 and 229 [*NWT Rules*]; Nunavut *Rules of the Supreme Court*, NWT Reg 010-96 (Nu) r 219, 225 and 229 [*Nu Rules*]; *Nova Scotia Rules*, *supra* note 5; Prince Edward Island, *Supreme Court Rules of Civil Procedure* [*PEI Rules*] , r 30.02; Saskatchewan *The Queen's Bench Rules*, S Gaz, December 27, 2013, 2684, Part 5 [*Saskatchewan Rules*]; Quebec *Code of Civil Procedure*, CQLR c C-25, s 401-403 [*Quebec Code*]; Yukon *Rules of Court*, YOIC 2009/65, r 25 [*Yukon Rules*]; *Tax Court of Canada Rules (General Procedure)*, SOR/90-688a, r 78 and 80 [*Tax Court Rules*]; and *Federal Courts Rules* (SOR/98-106), r 222 and 223 [*Federal Court Rules*].

11. Definitions of "document" are found at the following sections in the respective province's rules: *Ontario Rules*, *supra* note 10, r 30.01; *BC Rules*, *supra* note 10, r 1; *Manitoba Rules, supra* note 10, r. 30.01; NB Rules, *supra* note 10, r 31.01; *NWT Rules*, *supra* note 10, r 218; *Nu Rules*, *supra* note 10, r 218; *Yukon Rules*, *supra* note 10, r 1 (8); *PEI Rules*, *supra* note 10, r 30.01; *Saskatchewan Rules,* Part 17; Quebec, *An Act to establish a legal framework for information technology*, RSQ c C-1.1 [*Quebec Information Technology Act*], s 3; *Tax Court Rules*, *supra* note 10, r 78; *Federal Courts Rules*, *supra* note 10, r 222(1).

demanded rigorous adherence to best practices in the handling of electronic evidence. At the same time, some litigants found the discovery of ESI to be costly and burdensome. A precursor to these *Principles* was the document titled *Guidelines for the Discovery of Electronic Documents in Ontario* (the "Ontario E-Discovery Guidelines").[12] The introduction to that document noted that the "rules and the case law to date provide little clear guidance to parties and their counsel on how to fulfill that [e-discovery] requirement." This situation was not limited to Canada.[13]

In brief, attempts to apply the then existing discovery principles from the former paper-based age to the world of electronic information proved to be problematic. The new issues that have arisen in the world of electronic information have required a new approach. This demand was met by the publication of these *Principles* in 2008, which courts across Canada have since adopted as a standard.[14]

---

12. Discovery Task Force, *The Supplemental Discovery Task Force Report* (October 2005), online: Ontario Bar Association <http://www.oba.org/en/pdf_newsletter/DTFFinalReport.pdf>. The Supplemental Report includes Guidelines for the Discovery of Electronic Documents in Ontario, prepared by the e-discovery sub-committee.

13. See *Williams v. Sprint/United Management Co.,* 230 FRD 640 at 651, 2005 US Dist. LEXIS 21966 (WL): "[T]he Court finds insufficient guidance in either the federal rules or case law, and thus relies primarily on the Sedona Principles and comments for guidance on the emerging standards of electronic document production. . . ."

14. See e.g. Newfoundland and Labrador: *GRI Simulations Inc. v. Oceaneering International Inc.*, 2010 NLTD 85 (CanLII); Nova Scotia: *Velsoft Training Materials Inc. v. Global Courseware Inc*., 2012 NSSC 295 (CanLII), [*Velsoft*]; British Columbia: *Liquor Barn Income Fund v. Mather*, 2011 BCSC 618 (CanLII); Alberta: *Innovative Health Group Inc. v. Calgary Health Region*, 2008 ABCA 219 (CanLII); New Brunswick: *Saint John (City) Conseil des fiduciaires du régime de retraite des employés c Ferguson*, 2009 NBBR 74 (CanLII); Manitoba:

E. The Overarching Principles: Proportionality and Cooperation between the Parties

To anyone approaching ESI for the first time—perhaps someone more familiar with traditional information sources and methods of disclosure—the world of ESI will present two immediate and significant challenges: volume and complexity. To address these challenges, there are two principles at the heart of the Working Group's e-discovery best practices as articulated in these *Principles*: proportionality (*see* Principle 2) and cooperation between parties (*see* Principle 4).

Proportionality. In order to cope with the problems associated with the ever growing volume and complexity of electronic documentation, most jurisdictions have incorporated a principle of proportionality into their rules of court. Proportionality relates to the question of how much time and effort a party should reasonably have to expend, in light of all relevant factors, to perform e-discovery. Every jurisdiction that has adopted ESI-related rules of procedure that impose affirmative obligations has adopted a proportionality principle. While all ESI is discoverable and parties have a duty to preserve, search and then produce what meets the relevant test for disclosure, no party should be expected to preserve, search and produce all, or specific problematic sets of, ESI where to do so would impose costs and burdens disproportionate to the value of the case or the probative value of the evidence in question, taking into account the availability of the same information from other sources.

Commonwealth Marketing Group Ltd. et al v. The Manitoba Securities Commission et al., 2008 MBQB 319 (CanLII).

For example, Ontario Rule 29.1.03 requires the parties to agree to a discovery plan that takes into account "[the] relevance, costs and the importance and complexity of the issues in the particular action."[15] The discovery plan shall also include "any other information intended to result in the expeditious and cost-effective completion of the discovery process *in a manner that is proportionate to the importance and complexity of the action*."[16] Ontario Rule 29.1 also requires that, "[i]n preparing the discovery plan, the parties *shall* consult and have regard to the document titled 'The Sedona Canada Principles Addressing Electronic Discovery' developed by and available from The Sedona Conference."[17]

Cooperation between the Parties. While the original *Principles* primarily discussed the "meet-and-confer" process, the Canadian experience has developed more significantly around the principle of ongoing cooperation and the development of a discovery plan. The idea of cooperation between counsel and parties extends well beyond the confines of a meeting, or series of meetings, to the transparent sharing of information in an effort to keep discovery costs proportionate and timelines reasonable. At The Sedona Conference Working Group 7 August 2014 Meeting in Toronto, there was a universal consensus that the "meet and confer" language in these *Principles* be replaced with "cooperation" and "collaboration."

The Ontario Rules are illustrative of this principle of cooperation. The same provisions that emphasize proportionality also require consultation and agreement between the parties at

15. *Ontario Rules*, *supra* note 10, r 29.1.03(3)(a).

16. *Ontario Rules*, *supra* note 10, r 29.1.03(3)(e) [emphasis added].

17. *Ontario Rules*, *supra* note 10, r 29.1.03(4) [emphasis added].

the outset of the litigation.[18] The purpose of such consultation and cooperation in jointly developing a discovery plan is to minimize the scope, complexity and attendant difficulties of e-discovery for the parties and the entire judicial system. The Ontario Rules relating to e-discovery illustrate the importance of proportionality and of ongoing consultation between the parties in the e-discovery process.

F. How are Electronic Documents Different from Paper Documents?

Exploring and understanding the differences between paper and electronic documents can reveal important factors that determine how ESI should be handled. It can allow courts and parties to break from past practice where appropriate, while still achieving the fundamental objective of securing the "just, most expeditious and least expensive" resolution of each dispute.[19]

1. Large Volume and Ease of Duplication

ESI is created at much greater rates than paper documents. As such, there are vastly more electronic documents than paper documents.

Electronic documents are more easily duplicated than paper documents. For example, e-mail users frequently send the same e-mail to many recipients. Recipients often forward messages. E-mail systems automatically create copies as messages are sent. Other software applications periodically and automatically make copies of data.

---

18. See e.g. *Ontario Rules*, *supra* note 10, r 29.1.03(2).

19. See e.g. *Tax Rules*, *supra* note 10, s 4(1).

2. Persistence—ESI is Hard to Destroy

Electronic documents are more difficult to dispose of than paper documents. A simple command to "delete" an electronic document still generally leaves the file on a storage device until it is overwritten. Until it is overwritten, the data still exists and may be recovered using forensic methods. If the original electronic storage device is handed over by the producing party to the receiving party, the receiving party may find and be permitted to use that "deleted" data. *In Prism Hospital Software Inc. v. The Hospital Records Institute,*[20] the defendants produced magnetic media on which the plaintiff was able to locate a series of files that, although "deleted," continued to exist. The persistence of ESI means that it accumulates without a custodian knowing that it is still available.

It may be easier and less expensive to recover destroyed electronic documents than destroyed paper documents. At times, computer forensic techniques may allow parties to recover or reconstruct deleted documents, even, in some cases, documents that appear to have been permanently deleted. However, this does not mean that parties responding to document requests will always be required to produce deleted data or data fragments. Generally, the expense and disruption caused by such techniques cannot be justified. Here, an analogy to paper is useful. A producing party is not required to produce papers that it threw away a year ago. In *Rowe Entm't Inc. v. The William Morris Agency Inc.*,[21] (a U.S. case) the Court held, "just as a party would not be required to sort through its trash to resurrect discarded paper documents, so it should not be obligated

20. *Prism Hospital Software Inc. v. The Hospital Medical Records Institute*, 1991 BCJ No 3732 (1991) 62 BCLR (2d) 393 (WL) (SC).

21. 205 FRD 421 at 431 (WL) (SDNY 2002).

to pay the cost of retrieving deleted e-mails." However, if established that material evidence has been destroyed or lost, requiring parties to bear the costs of recovering destroyed documents may be justified. (*See* Principle 6).

3. Dispersion of ESI

While paper documents will usually be found in a limited number of locations, ESI can reside in numerous locations: desktop hard drives, laptops, network servers, smart phones, tablets, CDs, backup tapes and even floppy disks. These sources will likely contain not only exact digital duplicates; they will also likely contain "near-duplicates" ("near-dupes")—for example, multiple drafts of a report or contract.

4. Dynamic, Changeable Nature of Much ESI

In the world of paper discovery, a document preservation order requiring that a corporate party freeze all of its documents is a manageable burden. Paper documents can be left in their files or copied if they need to be marked up. Personnel can suspend their practice of throwing away old files. With paper, inaction is usually enough to preserve the document.

In contrast, in the electronic context, freezing all electronic information could be catastrophic to a business. It is virtually impossible to "freeze" a company's entire set of ESI without effectively shutting down its entire computer system. Normal business operations involve the constant alteration of certain classes of data. Instead, a well-organized litigation hold is required. There are now reliable methods of implementing and maintaining a hold on potentially relevant information without disrupting the entire enterprise.

Managing the dynamic nature of ESI is an ongoing challenge throughout any e-discovery project. Unlike paper documents, some kinds of electronic information have dynamic features that change over time, often without the user even being aware of the changes taking place. Collaborative tools also allow file contents and metadata to change without any particular user being aware of the change.

Databases present a particular challenge in e-discovery, as most large enterprises run databases that are constantly being updated, whether through direct user input or automatically. For example, a chain store with multiple locations may have the accounting system at each location update a main system with daily sales information, and a warehouse inventory database is typically updated every time shipments of product are received or sent. The information in business operations databases can change by the minute. Deciding which version of the database is the appropriate one to preserve for discovery may be problematic. Pre-preservation interviews with the client's information technology department (IT) and business unit leaders can address many of these issues.

More common file types like word-processing files and spreadsheets also have dynamic features. Date and time metadata can change when a user opens, moves or copies a file. Files that have other files linked with them or embedded within them may change whenever the related file changes. To prevent these changes from occurring, data can be forensically preserved, collected, or both. It can then be processed so as to preserve a particular version, including its metadata, while making the file viewable in a review tool.[22]

22. Modern processing and review tools allow reviewers to view either an image of the file or a native version of the file. However, in both cases,

5. Metadata

Nearly all electronic documents contain information known as metadata, which presents unique issues for the preservation and production of documents in litigation. Metadata is electronic information stored within or linked to an electronic file that is not normally seen by the creator or viewer of the file. Typical and common metadata fields are DateCreated, DateSent, Author and FileLocation (i.e. the location of the document on the user's computer or device, on the server or in the user's mailbox). Metadata is generated by the operating system or the application. Some metadata is not accessible without special tools.

In most cases, metadata will have no material evidentiary value; it does not usually matter when a document was printed or who typed the revisions. There are situations where metadata may be necessary for authenticating a document or establishing facts material to a dispute, such as when a file was accessed in a suit involving theft of trade secrets. These cases, however, are rare in practice.

Metadata can be used to objectively code documents or to properly interpret the meaning of other data.[23] There is, however, a real danger that some metadata recorded by the computer may be inaccurate. This risk is most present with loose electronic files. For example, word-processing documents do not come with metadata accurately identifying many important

---

the original, unaltered metadata will have been extracted, preserved and loaded into the review tool alongside the native file and/or image.

23. E.g. spreadsheet formulas can be used to properly interpret a spreadsheet; "track changes" functionality in Microsoft Word can be used to observe changes made to a document during the drafting process. For a full discussion, see *infra*, Introduction, section F.8 (Advanced Technology Can Help to Organize, Search and Make Sense of ESI) and see *infra* note 27.

attributes or contents of the document (e.g. the signatory of the letter, the sender of a memorandum and the people receiving carbon copies (CC) of the letter). When a new employee uses a word-processing program to create a memorandum by using a memorandum template created by a former employee, the metadata for the new memorandum may incorrectly identify the former employee as the author. To capture the true date, author, recipient, subject line, etc., of a set of documents, the parties cannot rely on such metadata alone—this information often must be derived from the text of the electronic document itself.

E-mail metadata, on the other hand, is often accurate and extremely useful for litigation purposes. Unlike the metadata associated with loose electronic files, e-mail metadata (if collected properly) does accurately identify the e-mail's signatory ("From"), the recipients ("To" and "CC"), and the precise date and time sent ("DateTime").[24] These fields can be extracted and loaded into a review platform for efficient searching and review.

In their discovery planning, counsel should consider whether to exchange metadata. As the profession has come to understand more about what metadata is and how it can be of use, too many practitioners still improperly refuse to consider the possibility of exchanging it as part of a production.[25] It is important to consider both (a) whether the metadata will have any

24. DateTime information in e-mails, however, can present challenges as time zone information, though embedded in the e-mail metadata, is often not correctly processed or displayed. For example, when a collection of documents involves custodians from various time zones, the DateTime information may not be correct depending on the time zone selected when processing the documents.

25. Discussions between the parties to exclude "metadata" from production often focus on ensuring that "hidden data," such as track changes in

dispositive evidentiary value in the proceedings and (b) whether the metadata will be useful for organizing and making sense of a body of ESI. While the metadata itself may not be used at trial, it is certainly useful for the litigation process when deciding what to review and in what order.

In advance of production, parties should agree on which metadata fields they will provide to each other along with the documents. If questions are raised about authenticity or chain of custody, additional metadata can be provided.

6. Structured Data

Today's information technologies have yielded not just electronic files that look and function more or less like letters and memoranda; they include databases and other kinds of "structured data" files. Information in databases is not necessarily organized in a body that can be read in rows starting in the top left and ending in the bottom right. The information is broken up into constituent elements, which are stored in multiple tables, each with records and fields. A sales database, for example, will contain multiple variables (e.g. Organizations, People, Transactions and Invoices), and someone interested in what happened on a particular day can only learn this if multiple rows and columns from all of these tables are pulled together in the proper way.

Parties possessing or demanding access to databases should agree in advance whether to produce native database files or provide, for example, specific reports from the database

---

word documents and formula in spreadsheets, is not produced. When such documents are produced in printed or scanned form, this information is lost to the receiving party. Strictly speaking, however, this kind of information is part of the substantive content of the document and should be preserved and, if appropriate, produced.

routinely produced, based on particular queries that contain specified records and fields.

7. Obsolescence of Hardware and Software

Electronic data, unlike paper data, may be incomprehensible when separated from the software within which it is created and used. Organizations upgrade their systems, sometimes rendering older files unreadable. People who know how to use the old system leave the organization and cannot be located. Software companies stop offering support for earlier versions of their software. In these situations, only reasonably accessible data need be produced, with "reasonably" being interpreted in light of all of the factors that affect proportionality. (*See* Principle 5).

8. Advanced Technology Can Help to Organize, Search and Make Sense of ESI

Working with ESI, while the volumes may far exceed those in the world of paper, is far more efficient than working with paper could ever be. Modern digital technologies, especially search and text classification tools, are extremely powerful, making it possible to organize, search and make sense of vast amounts of information in manageable amounts of time.

When reviewing paper documents before production, lawyers and paralegals commonly review each page of a document to see if the document mentions a person or event relevant to the issues in the pleadings. This practice need not be adopted with electronic files. In fact, it is inadvisable to print out electronic files to do a page-by-page review, as this entails the loss

of valuable information, including metadata, which could otherwise be used to organize, sort, search and make sense of the original "native" file.[26]

It is now possible to search ESI *in situ*, without the need for collection and removal to another location. On-site identification and culling prior to collection can be an effective means of reducing data volumes, with benefits at all later stages. Advance discussions with clients and cooperation with other parties is strongly encouraged. Proper forensic methods should be employed and soliciting the advice or involvement of experienced e-discovery professionals is strongly advised.

De-duplication technology can now eliminate significant volumes of ESI early in the process. With paper (and scanned images of paper), it was almost impossible to know that several reviewers were encountering copies of the same document. With ESI, de-duplication is easily accomplished, obviating the need for redundant review and, even worse, the risk of inconsistent review decisions. Near-duplicate detection allows similar documents to be grouped for more efficient review. E-mail threading organizes e-mails into conversations and identifies e-

26. "Native" is the term used to describe an electronic file in its original state, capable of being opened and viewed in the application that created it, with all the features it first possessed in that format. Thus, a Word document remains in its native format until it is printed or converted, for example to TIF or PDF format. A PDF is almost always a derivative of another (native) format, since most PDFs are generated from a preexisting e-mail, word-processing, spreadsheet, presentation, or other formats. But the fact that a file looks like a native file (if it has a .docx extension, for example) is not in itself proof that this is the original native file: someone can take a richly-formatted Word document, save it to plain-text format and then open it again in Word. It is no longer in its native format, even though it is now (again) in Word. It has lost much of its original content. Only the first Word file, with all its content and formatting, is the true native file.

mails whose content is wholly contained in other e-mails (and which can thus be suppressed from review), making review far more efficient.

It is now possible, using Technology Assisted Review (TAR), for lawyers to perform basic responsiveness coding and even issue-coding on a far greater body of documents than they could have reviewed manually.[27] This is accomplished having

27. The term "coding" is important in both paper-based and electronic discovery. It always refers to the assignment to a document of either (a) a piece of information that captures a property of the document or (b) a designation that reflects a judgment about the document. Coding is not applied to the face of the document; instead, it is stored as values in a database field linked to the document record. These fields are searchable, allowing users to find documents by specifying coding values—e.g. <Document Date falls after 1/1/2012>; <Author contains "Smith">; or <Attorney coding is "Relevant">. There are two mutually-exclusive kinds of coding: objective and subjective.

1. Objective Coding. Also known as bibliographic, or "bib", coding, objective coding comprises any factual information about the document that is not subject to interpretation or debate, such as DateSent, Author, Recipient and Title. Much of this objective information will be on the face of the document (DateReceived, Author, Subject), but often it is not (it is a letter; it is a fax cover page; it has four attachments). To perform objective coding is to determine which facts about a document are pertinent for the review and to populate database fields with the appropriate values so that the document record now contains that additional information. The term "objective coding" refers to both the act of coding and the body of searchable information created by the coding exercise. With paper or scanned documents, all objective coding must be created manually. With electronic documents, much of the objective *information* is found in metadata (E-mail Sender, DateSent, E-mail Subject), i.e. it is embedded in the electronic document. But with electronic files, much relevant information is not stored in metadata; objective coding may be necessary or desired, such as for word-processing documents in which the Author of a letter or the Subject of a Memorandum is not available in metadata. This helps to explain why metadata is not generally included in

one or a handful of subject-matter experts (SMEs—usually partners or senior associates who know the case extremely well) review subsets of documents, code them and then use this coding to "teach" the software what kinds of documents are wanted and not wanted. The software codes the rest of the documents, and then the team takes a sample of these results and checks to see if the system properly coded those documents. The SME decisions confirming or overturning the software's decisions are then fed back into the system. After a few iterations (SME coding, processing, sampling, SME coding. . .), a final result is achieved on the entire collection with a degree of statistical accuracy greater than could be hoped for in a traditional linear review by human coders. This technology has now met with judicial approval in the U.S.[28] While not yet widely adopted in

---

the concept "coding": "coding" connotes the act of capturing what is not already there and entering it into a database where it is searchable.

2. Subjective coding. This is the assigning to a document (traditionally, using Post-Its, but now by adding values to the document record in a review database) a reviewer's assessment of the significance of that document. Subjective coding captures a subjective judgment. Common subjective coding fields are Relevance, Issues and Privilege. While it is common for parties to exchange at least some objective fields (whether derived from metadata or created through manual coding), it is uncommon for them to exchange subjective coding. The latter will often constitute work product that could reveal the thoughts and impressions of counsel and which therefore enjoys protection from disclosure. See *infra*, Principle 9.

3. Predictive coding. The word "coding" now has a new connotation derived from recent machine learning applications. "Predictive coding" involves computers processing the text of large numbers of documents and, based on algorithms, assigning a score or a binary value to each document in an attempt to imitate or predict human subjective judgment. For a discussion of predictive coding, see *infra*, Comment 7.c.iv.

28. See e.g. *Da Silva Moore v. Publicis Groupe*, 287 FRD 182 (WL) at 192 (SDNY 2012), aff'd sub nom. *Moore v. Publicis Groupe SA*, 2012 US Dist. LEXIS 58742 (SDNY 2012) (Carter, J).

Canada, this illustrates the power and the potential of modern technology as a tool for efficiently and effectively managing ESI in litigation.

9. The Risk of Inadvertent Disclosure of Sensitive Documents

In the world of paper, the generally smaller document volumes coupled with an inability to perform searches make a linear "eyes-on" review of all documents eligible for production the appropriate means of guarding against the disclosure of sensitive information.[29] With ESI, the much larger volumes make linear review all but impossible (and cost-prohibitive in many cases), while modern electronic search technologies offer an alternative: searches that can find many if not most of the sensitive documents. But clients and counsel need to understand the inherent limitations of any kind of search technology and be alert to the risks of inadvertent disclosure that persist, and can even be accentuated, through the use of electronic search methods.

First, it is all but impossible to craft a set of search terms that will find, in a targeted and efficient way, all of the sensitive documents being sought.[30] Such a search will (a) return documents that are not in fact sensitive despite containing one or

29. The term "sensitive" is meant to encompass all reasons for either withholding entirely or redacting a document, including: all forms of privilege, the work product doctrine, commercially sensitive information, personal health information, personally identifiable information, and so on.

30. A common practice in the search for documents that might warrant a claim of solicitor-client privilege is to search the presumptive production population for the names of lawyers and law firms. Such a search will guarantee that any documents that are privileged and that contain one or more of these names will be pulled back, but it will also (1) pull back large numbers of documents that are not privileged despite containing these

more terms ("false positives") and (b) fail to identify documents that are or might be sensitive despite the lack of any of these terms ("false negatives"). The goal of any information retrieval exercise is to reduce the rate of false negatives (i.e. to find as many of the desired documents as possible) without also returning too many false positives. This remains a challenge for all forms of information retrieval but it is particularly acute in the world of legal search because of the risks involved.[31]

Second, it is essential when using automated search techniques against ESI to understand what is and is not being searched. The most important distinction here is between the "body" of a document and its metadata. The body of a document and its metadata are commonly separated from each other during processing and loaded into separate database fields in a review tool. At the same time, most review tools will build a standard "extracted text" index that only includes the body of

---

names and also (2) fail to pull back documents that might be privileged but do not contain any of these names. The first problem (low precision) results in increased review time; the second (low recall) represents the risk of inadvertent disclosure. To reduce this second risk (generally felt to be more acute), review teams will often include in their searches additional terms thought to be strong indicators of potential privilege, such as: law, lawyer*, legal, lawsuit*, privilege*, confidential*, damages, plaintiff, etc. But each of these terms will pull in false positives, particularly the terms privilege* and confidential*, which will find all e-mails that contain a standard automated disclaimer containing one or both of these terms.

31. It is always possible to reduce the risk of inadvertent disclosure by simply reviewing more documents. But searches that include more terms, or more permissive terms (e.g. using wildcards, stemming and fuzzy searching) to get closer to finding all potentially sensitive documents will almost always bring back larger and larger numbers of false positives. Reducing false negatives will increase "recall," thereby lowering the risk of inadvertent disclosure, but almost always at the cost of reduced "precision," which means increased review costs.

each document. A simple keyword search will thus, most likely, search only the body of e-mail messages and the visible content of non-e-mail files. It will not search the "e-mail header fields"[32] or any other metadata fields, such as Filename or the Folder Path from which a file was collected. As a result, unless indexes or the searches themselves are designed to avoid this risk, searches will most likely not return documents that the review team needs to see. Conversely, if these sorts of metadata fields are included in searches, results may be over-inclusive—such as when a search for a person's name returns all of that person's e-mails or when a search for a company name returns all the contents collected from a folder structure on the server. All of these factors should be kept in mind when performing searches to identify potentially sensitive information.

Clients and counsel need to understand both the benefits and the limitations of automated search methods, and seek advice where appropriate.

32. This term is generally used to refer to the From, To, Cc, Bcc and Subject fields.

II. PRINCIPLES AND COMMENTARY

Principle 1: Electronically stored information is discoverable.

Comment 1.a. Definition of Electronically Stored Information

While the rules of court in Canadian jurisdictions provide varying definitions of what constitutes a "record" or "document" for the purposes of production in discovery, they all provide that ESI must be produced as part of the discovery process. Typical forms of ESI include, but are not limited to, Word, PowerPoint, and Excel documents, e-mail, instant messages, databases, information on social media, and information posted on the internet.

The *Personal Information Protection and Electronic Documents Act*,[33] defines "electronic document" as "data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, print-out or other output of that data." The *Canada Evidence Act*[34] defines an electronic record or document as "data that is recorded or stored on any medium in or by a computer system or other similar device."

Quebec passed *An Act to Establish a Legal Framework For Information Technology*,[35] which includes the following definition:

33. SC 2000, c 5. [*PIPEDA*].

34. RSC 1985, c C-5, s 31.8. [*Canada Evidence Act*].

35. *Quebec Information Technology Act*, *supra* note 11.

> "Document": Information inscribed on a medium constitutes a document. The information is delimited and structured, according to the medium used, by tangible or logical features, and is intelligible in the form of words, sounds or images. The information may be rendered using any type of writing, including a system of symbols that may be transcribed into words, sounds or images or another system of symbols.

Comment 1.b. Relevancy

Canadian courts have repeatedly held that ESI is producible and compellable in discovery.[36] Rules of court make relevancy a prerequisite to production, regardless of the form of record. For example, Part Five, Rule 5.2(1) of the *Alberta Rules of Court*[37] provides that producible records be both relevant and material. The Ontario *Rules of Civil Procedure*[38] provide that every document relevant to any matter in question in the action shall be produced. The British Columbia rules were amended in

---

36. See *Cholakis v. Cholakis*, [2000] MJ No 6 at para 30, 44 CPC (4th) 162 (CanLII) (Man QB): "The plaintiff has satisfied me that the electronic information requested falls within the definition of a document under the Rules and contains relevant information that should be produced. If the defendants. . .wish to provide the information in a format that does not reveal irrelevant information, then it is incumbent upon them to develop a mechanism by which that can be done. The interests of broad disclosure in a modern context require, in my view, the production of the information in the electronic format when it is available."

37. *Alberta Rules, supra* note 10.

38. *Ontario Rules, supra* note 10, r 30.02 (1): Every document relevant to any matter in issue in an action that is or has been in the possession, control or power of a party to the action shall be disclosed as provided in rules 30.03 to 30.10, whether or not privilege is claimed in respect of the document.

2009 to introduce concepts of proportionality and narrow the scope of documentary discovery.[39]

Courts have ordered the production of actual media in particular cases, such as in *Reichmann v. Toronto Life Publishing Co.*,[40] where a party was ordered to produce not only a printed copy of a manuscript stored on a disk and already produced, but the disk itself. The Court found that the disk fell within the common law definition of a "document" and therefore had to be produced.

In *Northwest Mettech Corp. v. Metcon Service Ltd.*,[41] however, the Court declined to order production by the defendants of an entire hard drive, and ordered production of only the relevant data stored on the drive. The Court found that the drive was simply a storage medium or electronic filing cabinet containing electronic documents, and that the defendants were not required to list the entire contents or produce the entire electronic filing cabinet any more than they would be with respect to a filing cabinet containing paper. The Court did order the defendants to produce an affidavit verifying all of the files on the hard drive related to the matter in issue. In appropriate circumstances, with proper safeguards for privilege and confidentiality, a court may be willing to grant access to a hard drive or other medium, and/or to allow inspection.[42] This suggests that access for forensic purposes such as recovering deleted information may be permitted.

39. See *BC Rules, supra* note 10.

40. 66 OR (2d) 65 (HCJ), 1988 CanLII 4644 (ON SC).

41. 1996 CanLII 1056 at para 10 (BCSC).

42. See *Nicolardi v. Daley*, [2002] OJ No 595 at para 5 (ONSC) (QL).

Comment 1.c. E-Commerce Legislation and Amendments to the Evidence Acts

Most provinces have passed legislation that provides guidance for the use of electronic means for creating and managing records, and for electronic commerce transactions.[43] These statutes provide that information shall not be denied legal effect or enforceability solely by reason that it is in electronic form.

The statutes do not require individuals to use or accept information in electronic form, but the consent of a person to do so may be inferred from the person's conduct. Requirements that information be in writing are generally satisfied if the information is accessible so as to be useable for subsequent reference.

Currently, legislation across Canada provides a means to facilitate the admissibility of ESI in the courts, including the establishment of evidentiary presumptions related to integrity of electronic information and procedures for introducing such evidence and challenging its admissibility, accuracy and integrity. The legislation generally does not modify any common law or statutory rule related to the admissibility of records, except the rules relating to authentication and best evidence.[44]

---

43. The Yukon, Prince Edward Island, Ontario, Newfoundland, Nova Scotia and Nunavut have respectively passed: *Electronic Commerce Act*, RSY 2002, c 66; RSPEI 1988, c E-4.1; SO 2000, c 17; SNL 2001, c.E-5.2; SNS 2000, c 26; and SNu 2004, c 7. Alberta, New Brunswick, British Columbia and the North West Territories have similar legislation under the title of the *Electronic Transactions Act*, found respectively at: SA 2001, c E-5.5; RSNB 2011, c 145, SBC 2001, c 10, and SNWT 2011, c 13. Manitoba's legislation is titled: *Electronic Commerce and Information Act*, CCSM 2000 c E55. Saskatchewan's legislation is entitled: *Electronic Information and Documents Act*, SS 2000, c E-7.22. Quebec's legislation is: *Quebec Information Technology Act*, *supra* note 11.

44. See e.g. *Evidence Act*, RSO 1990 c E.23, s 34.1 [*Ontario Evidence Act*]; *Quebec Information Technology Act*, *supra* note 11, s 5, 6 and 7.

Principle 2: In any proceeding, the parties should ensure that steps taken in the discovery process are proportionate, taking into account: (i) the nature and scope of the litigation; (ii) the importance and complexity of the issues and interests at stake and the amounts in controversy; (iii) the relevance of the available electronically stored information; (iv) the importance of the electronically stored information to the Court's adjudication in a given case; and (v) the costs, burden and delay that the discovery of the electronically stored information may impose on the parties.

Comment 2.a. The Role of Proportionality

Proportionality is the "reasonableness" principle applied to the question of how much time and effort a party should have to expend with respect to ESI in light of all relevant factors. Courts across the country, including the Supreme Court of Canada, have confirmed that the principle of proportionality is to play a significant role in case management.[45] Every jurisdiction in Canada that has adopted ESI-related rules of procedure that impose affirmative obligations (e.g. ESI is discoverable, parties have a duty to preserve it, search it and produce what meets the threshold for disclosure) has adopted a proportionality principle.

The principle of proportionality is a reaction to delays and costs impeding access to justice, and while it requires a shift in legal culture, the intent of the principle is to create a new

45. See e.g. *Marcotte v. Longueuil (City)*, 2009 SCC 43 (CanLII); *Total Vision Enterprises Inc. v. 689720 BC Ltd*, 2006 BCSC 639 (CanLII) at para 36; *Abrams v. Abrams*, 2010 ONSC 2703 (CanLII).

norm. Master Short's decision in *Siemens Canada Limited v. Sapient Canada Inc.*,[46] provides an important analysis of proportionality and expectations of counsel to comply with this new principle.[47] This decision is referenced throughout these *Principles* and provides guidance for discovery planning and the transparency required by counsel in meeting their obligations.[48]

ESI is discoverable, and parties have a duty to preserve, search and then produce what ESI meets the relevant test for disclosure. But no party is required to preserve, search and produce all (or particularly problematic sets of) ESI where to do so would impose costs and burdens disproportionate to the value of the case or the probative value of the evidence in question, taking into account the availability of the same information from other sources and other factors. Proportionality principles are often used by a party seeking to reduce disclosure obligations, sometimes appropriately and sometimes inappropriately.

---

46. *Siemens Canada Limited v. Sapient Canada Inc.*, 2014 ONSC 2314 (CanLII) at para 51 [*Siemens*]. In *Siemens*, the parties did not establish a discovery plan but proceeded to produce documents without communicating with each other. When Siemens produced 120,043 documents, and Sapient only produced 23,356 documents, Siemens challenged Sapient's document production as deficient. While Siemens was partially successful on its motion, the Ontario Superior Court of Justice denied it any costs, noting that the parties were "the authors of their own misfortune" for proceeding without a discovery plan.

47. See also detailed analyses in: *Warman v. National Post Co* 2010 ONSC 3670 (Master Short) [Warman]; Kaladjian v. Jose, 2012 BCSC 357 (Davies, J) [Kaladjian]; The Sedona Conference, *The Sedona Canada Commentary on Proportionality in Electronic Disclosure & Discovery* (Oct. 2010 public comment version) and its Appendix 1, online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/468>.

48. *Siemens*, *supra* note 46. See also <http://www.felsky.com/blog/ontario-master-proportionality-requires-transparency> for a discussion on the key points of the decision.

The widespread use of computers and the internet has created vast amounts of ESI, making the cost and burden of discovery exponentially greater than it was in the "paper" world. Even a case involving small dollar amounts and straightforward legal issues can give rise to significant volumes of ESI. Litigants should take a practical and efficient approach to electronic discovery, and should ensure that the burden of discovery remains proportionate to the issues, interests and money at stake. Without a measured approach, overwhelming electronic discovery costs may prevent the fair resolution of litigation disputes. "The new *Rules* recognize that application of a 19th century test to the vast quantity of paper and electronic documents produced and stored by 21st century technology had made document discovery an unduly onerous and costly task in many cases. Some reasonable limitations had become necessary and Rule 7-1 (1) is intended to provide them."[49]

The case law underscores that "proportionality is a parsimonious principle."[50] That is, the proportionality principle should generally lead to a narrowing, not an expansion, of the volume of discovery. That being said, parties should not use the proportionality principle as a shield to avoid their legitimate discovery obligations. Parties should plan for the e-discovery process from the outset with a view to analyzing the potential costs of e-discovery, the means of controlling such costs and what process might best achieve proportionality.[51] As stated by

---

49. *Kaladjian, supra* note 47 at para 60, citing N. Smith J in *More Marine Ltd. v. Shearwater Marine Ltd.*, 2011 BCSC 166.

50. *Ontario v. Rothmans Inc.*, 2011 ONSC 2504 (CanLII) at para 160.

51. See e.g. *L'Abbé v. Allen-Vanguard*, 2011 ONSC 7575 (CanLII) at para 24: "efficiency and cost effectiveness in production and discovery should be a mutual goal. Questions of relevance and privilege must be answered of course but it is necessary to apply those filters in a practical manner . . . .

the Court in *Siemens*: "[n]ow as we approach the fifth anniversary of the Rule changes, a case such as this presents an opportunity to demonstrate the consequences of postponing the development of a practical discovery plan and to stress the obligation of the parties and counsel to define the basis upon which both parties will establish their productions in complex cases such as this."[52]

Costs extend beyond recovering electronic documents or making them available in a readable form, searching documents to separate the relevant material from the irrelevant material, reviewing the documents for privilege and producing the documents to the other party. Non-monetary costs and other factors include possible invasion of individual privacy as well as the risks to confidences and legal privileges. Electronic discovery can overburden information-technology personnel and organizational resources.

Courts frequently balance the costs of discovery with the objective of securing a just, speedy and inexpensive resolution of the dispute on the merits.[53] In the discovery context, Canadian courts have begun to emphasize their mandate to meet that objective.[54] Courts have not ordered production of documents where the parties have demonstrated that the costs of producing documents or the adverse effect upon other interests, such as

---

Equally or more important is the need for collaborative and creative goal oriented problem solving by the parties and their respective counsel."

52. *Siemens, supra* note 46 at para 51.

53. The rules of court in every jurisdiction in Canada contain a provision emphasizing the overriding importance of maintaining proportionality within legal proceedings.

54. See e.g. *L'Abbé, supra* note 51 at para 41.

privacy and confidentiality, outweigh the likely probative value of the documents.[55]

It has also been suggested that discovery disputes need to be proportionate and not themselves be an occasion for adversarial advocacy, and alternate forms of adjudication such as a reference under Ontario's Rule 54.03 may be appropriate.[56] At least one Justice of the Ontario Superior Court of Justice included proportionate electronic discovery and planning in his standard Case Management Directions.[57] Proportionality applies not only to the parties' use of their own resources, but also to their use of the Court's time.[58]

---

55. *Goldman, Sachs & Co. v. Sessions*, 2000 BCSC 67 (CanLII) (declining to order production where probative value outweighed by time and expense of production and the party's confidentiality interest); *Ireland v. Low*, 2006 BCSC 393 (CanLII) [*Low*] (declining to order production of hard drive where probative value outweighed by privacy interests); *Baldwin Janzen Insurance Services (2004) Ltd. v. Janzen*, 2006 BCSC 554, 53 BCLR(4th) 329 [*Janzen*] (CanLII) (declining to order production of hard drive in the particular circumstances of the case); *Desgagne v. Yuen*, 2006 BCSC 955, 56 BCLR(4th) 157 (CanLII) (declining to order production of a hard drive, metadata and internet browser history due, in part, to the intrusive nature of the requested order compared to the limited probative value of the information likely to be obtained.).

56. *Siemens, supra* note 46 at para 40; *Lecompte Electric Inc. v. Doran (Residential) Contractors Ltd.*, 2010 ONSC 6290 (CanLII) at para 15.

57. See e.g. *Yan v. Chen*, 2014 ONSC 3111 at Appendix A (CanLII) (Brown J).

58. *Sherman v. Gordon*, 2009 CanLII 71722 (ON SC) ("The concept of proportionality has to apply in the context of the litigants' use of court time as well as to the expenditure of their funds.").

Comment 2.b. The Proportionality Rule by Jurisdiction

As noted above, in the last few years, most Canadian jurisdictions have amended their respective rules of court to expressly include proportionality as a general rule for all litigation, and specifically in discovery procedures.

The Chief Justice of the Supreme Court of British Columbia promulgated a *Practice Direction Regarding Electronic Evidence* (effective July 1, 2006),[59] setting forth default standards for the use of technology in the preparation and management of civil litigation, including the discovery of documents in electronic form (whether originating in electronic form or not). Section 6.1 suggests that the scope of discovery may be modified to reflect the circumstances of the particular case. For example, it requires the parties to confer regarding limitations on the scope of electronic discovery where the ordinary rules would be "unduly burdensome, oppressive or expensive having regard to the importance or likely importance" of the electronic documents.[60]

In Nova Scotia, the requesting party must establish a *prima facie* case that something relevant will be uncovered. The Court has authority to limit discovery. For example, in *Nova Scotia (Attorney General) v. Royal & Sun Alliance Insurance Co. of Canada*,[61] the Court observed: "there is a discretion to limit discovery where it would be just to do so, such as where the burdens

59. Courts of British Columbia, *Practice Direction Re: Electronic Evidence* (2006), online: Courts of British Columbia <http://www.courts.gov.bc.ca/supreme_court/practice_and_procedure/practice_directions_and_notices/electronic_evidence_project/Electronic%20Evidence%20July%201%202006.pdf> [*BC Practice Direction*].

60. *Ibid.*

61. 2003 NSSC 227 at para 8, 218 NSR(2d) 288 (CanLII).

that would be placed upon the party making answer clearly outweigh the interests of the party questioning."

In Quebec, Section 4.2 of the *Code of Civil Procedure* (CCP) reads as follows: "In any proceeding, the parties must ensure that the proceedings they choose are proportionate, in terms of the costs and time required, to the nature and ultimate purpose of the action or application, and to the complexity of the dispute; the same applies to proceedings authorized or ordered by the judge."[62] Quebec courts have indicated that the proportionality rule must be interpreted in conjunction with section 4.1 CCP.[63] Section 4.1 reads as follows: "Subject to the rules of procedure and the time limits prescribed by this Code, the parties to a proceeding have control of their case and must refrain from acting with the intent of causing prejudice to another person or behaving in an excessive or unreasonable manner, contrary to the requirements of good faith." The rule of proportionality has been applied to the exchange of documents on CDs,[64] to the examination of a witness by videoconference[65] as well as to the control of an examination where an excessive volume of documents had been requested and an unreasonable number of questions had been asked.[66] Although "the Court sees to the orderly progress of the proceedings and intervenes to ensure proper manage-

62. RSQ c C-25, s 4.2.

63. *9103-3647 Québec Inc. c Couët*, 2003 IIJCan 14311 (CanLII) (QC CS).

64. *Citadelle, Cie d'assurance générale c Montréal (Ville)*, 2005 IIJCan 24709 (CanLII) (QC CS).

65. *Entreprises Robert Mazeroll Ltée c Expertech - Batisseur de réseaux Inc.*, 2005 IIJCan 131, 2005 CarswellQue 9122 (QC CQ).

66. *Ryan Parsons c Communimed Inc.* (2005), JE 2005-1042, 2005 CarswellQue 2058 (WL) (CQ).

ment of case" according to section 4.1 CCP para 2, the application of the proportionality rule relies on the parties, as stated by section 4.2 CCP.[67]

The proportionality principles in the Ontario *Rules of Civil Procedure* and the *Sedona Canada Principles* have also been adopted in interpreting procedural rules in other forums, including Ontario's Financial Services Tribunal.[68]

Comment 2.c. An Evidentiary Foundation for Proportionality

When a producing party wishes to reduce the scope of its production obligations by relying on the proportionality principle, or when a requesting party seeks to compel the responding party to expand its document disclosure, that party must lead evidence.[69]

In Ontario, the E-Discovery Implementation Committee has prepared a model chart to assist parties to argue production

---

67. Luc Chamberland, *La Règle de proportionnalité: à la recherche de l'équilibre entre les parties?* in La réforme du Code de procédure civile, trois ans plus tard (Cowansville, Que: Yvon Blais, 2006).

68. *BCE Inc. v. Ontario (Superintendent of Financial Services)*, 2012 ONFST 25 (CanLII) and *Rakosi v. State Farm Mutual Automobile Insurance Co.*, 2012 CarswellOnt 7066 (ONFSC Appeal decision).

69. See e.g. *Midland Resources Holding Limited v. Shtaif*, 2010 ONSC 3772 (CanLII) at para 15 ("at least some evidence"); *Dell Chemists (1975) Ltd. v. Luciani et al*, 2010 ONSC 7118 at para 5 (CanLII) ("cogent evidence"); *Saliba v. Swiss Reinsurance Co.* , 2013 ONSC 6138 (CanLII) (appeal from Master); *Velsoft*, *supra* note 14 at para 8; *Siemens*, *supra* note 46 at paras 142–144; *BCE*, *supra* note 68 at para 35; *Hudson v. ATC Aviation Technical Consultants*, 2014 CanLII 17167 (ON SC) [*ATC Aviation*] (appeal of Master's decision) at para 13; and *Kaladjian, supra* note 47 at paras 62–64. But see *Rothmans, supra* note 50 at para 164**.**

motions based on proportionality.[70] The case law supports the use of the chart to structure proportionality arguments.[71]

Comment 2.d. Proportionality in Procedure

While the focus of these *Principles* is to provide an outline of best practices with respect to the handling of ESI, it is important to note briefly the broader role proportionality has in civil litigation and the required shift in legal culture. In *Hryniak v. Mauldin*,[72] the Supreme Court of Canada discussed the role of proportionality in the Canadian civil justice system and the need for a shift in legal culture to maintain the goals of a fair and just process that results in a just adjudication of disputes.[73]

While the context of the decision was an appeal of a summary judgment motion, the Court discussed the developing consensus that extensive pretrial processes no longer reflect modern reality, and a new proper balance requires proportionate procedures for adjudication. As stated at paragraphs 28–29:

> The principal goal remains the same: a fair process that results in a just adjudication of disputes. . . . However, that process is illusory unless it is also accessible—proportionate, timely and affordable. The proportionality principle means that the best forum for resolving a dispute is not always that with the most painstaking procedure.

---

70. Ontario Bar Association, *Model E-Discovery and E-Trial Precedents* at "Materials for use by the Court-Model Document #10," online: Ontario Bar Association <http: //www.oba.org/en/publicaffairs_en/e-discovery/model_precedents.aspx>.

71. *Guestlogix v. Hayter*, 2010 ONSC 4384 (CanLII).

72. *Hryniak v. Mauldin,* 2014 SCC 7 (CanLII), [2014] 1 S.C.R. 87.

73. *Ibid* at paras 23–33.

> . . .
>
> If the process is disproportionate to the nature of the dispute and the interests involved, then it will not achieve a fair and just result.

Noting that the proportionality principle is reflected in many of the provinces' rules, the Court confirmed that proportionality can act as a touchstone for access to civil justice. Relying on a decision of the Newfoundland Court of Appeal,[74] the Court stated that even where the proportionality principle is not codified, rules of court that involve discretion include the underlying principle of proportionality, taking into account the appropriateness of the procedure, costs and impact on the litigation and its timeliness, given the nature and complexity of the litigation.

Most provinces have summary litigation procedures where the amount at issue is less than $100,000. For example, in British Columbia, Rule 68 of the Supreme Court Rules[75] modifies ordinary litigation procedures for certain actions to require the Court to consider what is reasonable where the amount at issue is less than $100,000. Rule 68 limits the times at which interlocutory applications may be brought and modifies the generally broad scope of discoverable documents. In particular, a party must list only those documents referred to in the party's pleading, the documents to which the party intends to refer to at trial, and all documents in the party's control that could be used to prove or disprove a material fact at trial. The Court has the discretion to require more extensive discovery, but will

74. *Szeto v. Dwyer*, 2010 NLCA 36, cited at *Hryniak*, *ibid* at para 31.

75. *BC Rules*, *supra* note 10; see also *Ontario Rules*, *supra* note 10, r 76, presenting a Simplified Procedure applicable to most civil actions involving less than $100,000.

"consider the difficulty or cost of finding and producing the documents."

Principle 3. As soon as litigation is reasonably anticipated, the parties must consider their obligation to take reasonable and good-faith steps to preserve potentially relevant electronically stored information.

Comment 3.a. Scope of Preservation Obligation

A party's obligation to preserve potentially relevant evidence will vary across jurisdictions and proceedings. Parties should understand their obligations with respect to the preservation/non-spoliation of evidence, including ESI.[76] For example, as set out below, in common law jurisdictions the obligation to preserve data arises as soon as litigation is contemplated or threatened, but when that point is reached is a fact-by-fact determination. If a company receives threats of litigation on a daily basis, having to preserve all data every time a letter is received would effectively mean that the company could never delete any documents. When this obligation arises is a legal question to be carefully considered in each case.

Due to volume, complexity, format, location and other factors, the possible relevance of collections of ESI or individual electronic files may be difficult to assess in the early stages of a dispute. Even where such an assessment is technically possible,

76. The obligations to preserve relevant evidence for use in litigation are distinct from any regulatory or statutory obligations to maintain records. For example, various federal and provincial business corporations' acts and insurance health statutes prescribe statutory requirements for record keeping. Records management and obligations to meet regulatory and statutory record keeping is outside the scope of *The Sedona Canada Principles Addressing Electronic Discovery*.

it may involve disproportionate cost and effort. In such circumstances, it may be more reasonable to expect a party to first make a good-faith assessment of where (in what locations; on what equipment) its relevant ESI is most likely to be found and then, with the benefit of this assessment, take appropriate steps to preserve those sources.

The general obligation to preserve evidence extends to ESI but must be balanced against the party's right to continue to manage its electronic information in an economically reasonable manner. This includes routinely overwriting electronic information in appropriate cases. It is unreasonable to expect organizations to take every conceivable step to preserve all ESI that may be potentially relevant.

Comment 3.b. Preparation for Electronic Discovery Reduces Cost and Risk: Information Governance and Litigation Readiness

The costs of discovery of ESI can be best controlled if steps are taken to prepare computer systems and users of these systems for the demands of litigation or investigation. Information governance is growing in importance, beyond just the realm of e-discovery, implicating virtually all operations of an organization. To reflect the importance of information governance and its "downstream" effects in an e-discovery engagement, the Electronic Discovery Reference Model (EDRM) incorporated Information Governance into its diagram in 2007[77] and has also developed an Information Governance Reference Model (IGRM).[78]

---

77. See EDRM, EDRM Diagram Elements, online: EDRM <http://www.edrm.net/resources/diagram-elements>.

78. The IGRM is more than an expansion of this one cell in the EDRM. See EDRM, Information Governance Reference Model (IGRM), online:

The possibility that a party will have to demonstrate that it used defensible methods in the handling of ESI and that it maintained proper chains of custody makes effective information governance practices all the more important. The integrity of electronic records begins with the integrity of the records management systems in which they were created and maintained.

With a view to litigation readiness, larger organizations should consider establishing an e-discovery response team, with representation from key stakeholders, including legal, business unit leaders, IT, records/information governance, human resources, corporate security and perhaps external e-discovery consultants / service providers.

The steps to be taken to ensure compliance with best practices and to control costs include defining orderly procedures and policies for preserving and producing potentially relevant ESI, and establishing processes to identify, locate, preserve, retrieve, assess, review and produce data. A records retention policy should provide guidelines for the routine retention and destruction of ESI as well as paper, and account for necessary modifications to those guidelines in the event of litigation.

EDRM <http://www.edrm.net/projects/igrm>. "The IGRM Project does NOT aim to solely build out the Information Management node of the EDRM framework. It will be extensible in numerous directions, such as records management, compliance and IT infrastructure." Principles and protocols about ESI and evidence have been published by various bodies across Canada, including the Canadian Judicial Council, the Canadian General Standards Board, the Competition Bureau <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03789.html>, and various provinces. The Sedona Canada Working Group favors continuing efforts to reach consensus on principles, protocols and best practices in information governance and e-discovery.

Having a records management system that provides a map of where all data is stored and how much data is in each location, and having an understanding of how difficult it is to access, process and search those documents will enable a party to present a more accurate picture of the cost and burden to the Court when refusing further discovery requests, or when applying for orders shifting costs to the receiving party in appropriate cases. It also mitigates the risk of failing to preserve or produce evidence from computer systems, thereby reducing the potential for sanctions. Costs can also be controlled through careful and cooperative discovery planning.

In *Siemens*, the defendant's corporate retention policy was considered inadequate and resulted in an order requiring further recovery attempts. The Court stated that "[o]bviously a company is entitled to establish whatever e-mail retention policies it wishes in order to minimize server use and cost. However, in a project such as this, which obviously carries over a lengthy period of time, such a policy can potentially create serious problems."[79]

Comment 3.c. Response Regarding Litigation Preservation

Parties should take reasonable and good-faith steps to meet their obligations to preserve information relevant to the issues in an action.[80] As noted above, in common law jurisdictions, the preservation obligation arises as soon as litigation is

79. *Siemens*, *supra* note 46 at paras 135–138.

80. *Doust v. Schatz*, 2002 SKCA 129 at para 27, 227 Sask. R 1 (CanLII): "The integrity of the administration of justice in both civil and criminal matters depends in a large part on the honesty of parties and witnesses. Spoliation of relevant documents is a serious matter. Our system of disclosure and

contemplated or threatened.[81] Owing to the dynamic nature of ESI, any delay increases the risk of relevant evidence being lost and subsequent claims of spoliation.[82] A proactive preservation plan will ensure a party can respond meaningfully and quickly to discovery requests or court orders.

---

production of documents in civil actions contemplates that relevant documents will be preserved and produced in accordance with the requirements of the law: see e.g. *Livesey v. Jenkins*, reflex, [1985] 1 All E.R. 106 (H.L.); *Ewing v. Ewing (No. 1)* (1987), 1987 CanLII 4889 (SK CA), 56 Sask. R. 260; *Ewing v. Ewing (No. 2)* (1987), 1987 CanLII 4865 (SK CA), 56 Sask. R. 263 (C.A.); *Vagi v. Peters*, reflex, [1990] 2 W.W.R. 170; *R. v. Foster and Walton-Ball* (1982), 1982 CanLII 2522 (SK CA), 17 Sask. R. 37 (C.A.); and *Rozen v. Rozen*, 2002 BCCA 537 (CanLII), [2002] B.C.J. No. 2192 (Q.L.). "A party is under a duty to preserve what he knows, or reasonably should know, is relevant in an action. The process of discovery of documents in a civil action is central to the conduct of a fair trial and the destruction of relevant documents undermines the prospect of a fair trial."

81. See *Culligan Canada Ltd. v. Fettes*, 2009 SKQB 343 (reversed on other grounds): "As soon as litigation was threatened in this dispute, all parties became obligated to take reasonable and good faith steps to preserve and disclose relevant electronically stored documents." In *Johnstone v. Vincor International Inc.*, 2011 ONSC 6005, a defendant was on notice that a legal action had been started, but chose to rely on a technicality regarding service and failed to follow its own policies in place to deal with situations of this nature when it knew that it had record retention policies in place that would possibly lead to the loss of important and relevant documents. The Court noted that as retention policies and preservation plans serve two different purposes, organizations may need to act promptly at the outset of possible litigation to suspend automatic electronic file destruction policies in order to preserve evidence.

82. On the issue of intentional spoliation of evidence as a separate tort, see *North American Road Ltd. v. Hitachi Construction*, 2005 ABQB 847 at paras 16–17, [2006] AWLD 1144; *Spasic Estate v. Imperial Tobacco Ltd., et al.* (2000), 49 OR (3d) 699 (CA), 2000 CanLII 17170. On the issue of the appropriate relief in connection with negligent spoliation, see *McDougall v. Black & Decker Canada Inc.*, 2008 ABCA 353 (CanLII).

In Nova Scotia, Rule 16 of the *Civil Procedure Rules* specifically outlines preservation requirements and refers to the obligations established by law to preserve evidence before or after a proceeding is started.[83]

The scope of what is to be preserved and the steps considered reasonable may vary widely depending upon the nature of the claims and information at issue.[84] The courts have ordered

---

83. *Nova Scotia Civil Procedure Rules*, Royal Gazette Nov 19, 2008, Part 5;

16.01:

> (1) This Rule prescribes duties for preservation of relevant electronic information, which may be expanded or limited by agreement or order.
>
> (2) This Rule also prescribes duties of disclosure of relevant electronic information and provides for fulfilling those duties . . .

16.02:

> (1) This Rule 16.02 provides for preservation of relevant electronic information after a proceeding is started, and it supplements the obligations established by law to preserve evidence before or after a proceeding is started.

16.14:

> (1) A judge may give directions for disclosure of relevant electronic information, and the directions prevail over other provisions in this Rule 16.
>
> (2) The default Rules are not a guide for directions.
>
> (3) A judge may limit preservation or disclosure in an action only to the extent the presumption in Rule 14.08, of Rule 14 — Disclosure and Discovery in General, is rebutted.

84. In contrast to the extensive case law and commentary in the United States, the law regarding preservation of electronic documents in Canada is still developing. Not surprisingly, several Canadian courts have looked to the U.S. for guidance in defining the scope of the duty to preserve, though

more targeted preservation.[85] That said, parties that repeatedly have to deal with preservation issues should consider what steps they can take to avoid having to repeat steps in the future.

Comment 3.d. Notice to Affected Persons in Common Law Jurisdictions—Legal Holds

Upon determining that a preservation obligation has been triggered,[86] the party should communicate to affected persons the need to preserve relevant information in both paper and electronic form. This notice is referred to as a "legal hold." The style, content and distribution of the legal hold will vary widely depending upon the circumstances, but the language used should be plain and clear and provide clear instructions to recipients. The legal hold should set out in detail the kinds of information that must be preserved so the affected custodians

---

U.S. law is more demanding than in Canada in notable respects. The decisions from the Southern District of New York in *Zubulake v. UBS Warburg LLC*, 220 FRD 212 at 217 (SDNY 2003) (WL) and *Pension Committee of the University of Montreal Pension Plan v. Banc of America Secs., LLC, et al.*, No 05 Civ 9016 (SAS), 2010 WL 184312 (SDNY 2010), provide guidance regarding the scope of the duty to preserve electronic documents and the consequences of a failure to preserve documents that fall within that duty. At paragraph 7 of the former, the Court commented as follows on the scope of the duty to preserve: "Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, 'no.' Such a rule would cripple large corporations, like UBS, that are almost always involved in litigation. As a general rule, then, a party need not preserve all backup tapes even when it reasonably anticipates litigation."

85. *Drywall Acoustic, Lathing and Insulation, Local 675 Pension Fund (Trustees) v SNC Lavalin Group Inc.*, 2014 ONSC 660 at paras 111–112 [*Drywall Acoustic*].

86. The Crown and police in criminal proceedings also have a duty to preserve evidence. See *R v. Sharma,* 2014 ABPC 131 (CanLII) at para 92.

can segregate and preserve it. Legal holds should not typically require the suspension of all routine records management policies and procedures. The legal hold should also advise the custodians that relevant documents can exist in multiple locations (i.e. networks, workstations, laptop, home computers, phones, tablets, voicemail, paper, etc.).

As noted above, the legal hold only needs to be sent to "affected" persons, i.e. those reasonably likely to maintain documents relevant to the litigation. Often custodian interviews will help to identify which people actually hold relevant documents. The legal hold should also be sent to the person(s) responsible for maintaining and operating the computer systems that house the documents subject to the legal hold. This is often the organization's IT department. A meeting should also be held with the IT people to ensure everyone understands what information must be preserved by the legal hold. The legal hold may, in certain cases, also be sent to non-parties who have in their possession, control or power information relating to matters at issue in the action.

The legal hold should mention the volatility of ESI and make it clear that particular care must be taken not to alter, delete or destroy it.[87] Once a legal hold is issued, this step is not over. It is advisable to resend the legal hold to the custodians at least every 6 months, and to ensure it is sent to any new employees to whom it may apply. While we have not seen any case law on this point yet in Canada, there is case law in the U.S. that requires legal holds to be resent on a regular basis. Custodians should also be advised when a legal hold is lifted. When legal

87. Ontario Bar Association, *Model E-Discovery and E-Trial Precedents* at "Materials for use by the Court-Model Document #5-6," online: Ontario Bar Association <http: //www.oba.org/en/publicaffairs_en/e-discovery/model_precedents.aspx>.

holds apply to documents and data spanning a significant or continuing period, organizations should determine how to deal with systems, hardware or media containing unique relevant material that might be retired as part of technology upgrades. Database information should also be considered.

> *Illustration i:* A company receives a statement of claim alleging that it has posted false or misleading information about its products on its website. It uses an outsourcer to manage its e-mail and its website. As part of its contract for services, the company requires the outsourcer to make weekly backups of the website and to keep the backup tapes for 6 months, after which it would keep the last copy of the month. The company issues a legal hold to the outsourcer asking it to suspend the rotation of the backup tapes until it can determine which tapes would contain the version of the website corresponding to the time period mentioned in the claim.
>
> *Illustration ii:* A former employee is suspected of having stolen client contact information and copies of design diagrams when he resigned to start a competing company. The relevant systems can generate electronic reports that can be sent by e-mail to a recipient. A legal hold should be sent to the company's IT department asking that it preserve the log of the former employee's activities as well as any e-mails sent, received or deleted from the former employee's account. The legal hold should also instruct the company's IT department

> from "wiping" the former employee's workstation and reassigning it to another member of the company.

The best evidence for the case in this illustration, however, may be with the former employee. See below discussion on Anton Piller orders in Comment 3.g. (Preservation Orders).

Comment 3.e. Preservation in the Province of Quebec

In the civil law jurisdiction of Quebec, the parties' obligations in the context of litigation differ from that in common law jurisdictions. For instance, the obligation to disclose documents to the opposing party ("communication of documents") is, at the first stage of litigation, limited to those documents that the disclosing party intends to refer to as exhibits at the hearing. The receiving party can also request specific documents in the context of discovery.

Although there is no specific obligation to preserve electronic documents in advance of litigation,[88] the Superior Court has recognized the existence of an implicit obligation to preserve evidence based on the general obligation of parties to refrain from acting with the intent of causing prejudice to another person or behaving in an excessive or unreasonable manner, which would be contrary to the requirements of good faith as prescribed by the *Code of Civil Procedure*.[89]

Before litigation has started, a party who has reason to fear that relevant evidence will become lost or more difficult to use can apply to the Court for an order to allow a person of their

88. *Jacques c Ultramar ltée*, 2011 QCCS 6020 (CanLII).

89. *Quebec Code*, *supra* note 10 at s 4.1.

choice to examine the evidence in question if its condition may affect the outcome of the expected legal proceeding.[90]

In Quebec, in view of the absence of an express preservation obligation, a party seeking a preservation order would need to present a motion for injunction or safeguard order in accordance with the criteria governing such proceedings.[91] In all circumstances, parties should send a legal hold letter to the other parties to ensure that the other parties are aware of the ESI that will be requested.

Comment 3.f. Extreme Preservation Measures Are Not Necessarily Required

The basic principle which defines the scope of the obligation to preserve relevant information can be found in the common law.[92] A reasonable inquiry based on good faith to identify and preserve active and archival data should be sufficient. In instances where relevant ESI can only be obtained from backup tapes or other non-readily accessible sources and the effort required to preserve them is not disproportionate given the issues and interests at stake, they should be preserved.[93]

In situations where deleted, fragmented or overwritten information can only be recovered at significant cost, a party may not be required, absent agreement or a court order based

---

90. *Ibid*, s 438.

91. *Ultramar, supra* note 88 at para 26.

92. The Ontario E-Discovery guidelines provide a useful resource: Discovery Task Force, *Guidelines for the Discovery of Electronic Documents* (2005) at Principle 3 and Principle 4, online: Ontario Bar Association <http://www.oba.org/en/pdf_newsletter/E-discoveryguidelines.pdf> [*Discovery Task Force Guidelines*].

93. *Mansfield v. Ottawa*, 2012 ONSC 5208 at para 43 (CanLII).

on demonstrated need and relevance, to recover and preserve such information. (See Principle 6).

Comment 3.g. Preservation Orders

In some cases it may be appropriate to seek the intervention of the Court to ensure that ESI is preserved. For example, Anton Piller orders,[94] which allow one party to copy or take custody of evidence in the possession of another party, have been widely used in most Canadian jurisdictions when one party is concerned that the opposing party will destroy relevant ESI. Anton Piller orders are exceptional remedies, granted without notice and awarded in very limited circumstances, for instance "when it is essential that the plaintiff should have inspection so that justice can be done between the parties. . . [and]. . .there is a grave danger that vital evidence will be destroyed." The Supreme Court of Canada provided guidelines for the granting and execution of Anton Piller orders in *Celanese Canada Inc. v. Murray Demolition Corp*.[95]

To avoid having a Court make a determination as to whether a sufficiently strong case has been presented for the granting of an Anton Piller order, the parties may choose to deal "cooperatively and in a common sense manner with the points of concern," as the parties did with respect to the motion brought by the plaintiffs for Anton Piller relief in *CIBC World Markets Inc. v. Genuity Capital Markets*.[96] The defendants voluntarily undertook to preserve the electronic evidence and retained a forensic consultant to execute the preservation. The

94. The order is named after the English case of *Anton Piller KG v Manufacturing Processes Ltd & Ors*, [1975] EWCA Civ 12, [1976] 1 All ER 779.

95. 2006 SCC 36 (CanLII).

96. 2005 CanLII 3944 (ON SC).

Court provided in its Order that the forensic consultant was to have access to the defendants' systems and devices so that it could image and store the contents of computers, Blackberries and other similar electronic devices the defendants had in their possession, power, ownership, use and control, both direct and indirect. The Court Order also provided that the forensic consultant was to have access to such devices wherever located, including at any office or home (but not restricted to such locations), regardless of whether the devices were owned or used by others.

In instances where intentional destruction of evidence is not an issue, the risk of inadvertent deletion can be addressed by a demand to preserve evidence.[97] An Anton Piller order obtained *ex parte* was set aside where the plaintiff did not establish a real possibility that evidence may be destroyed.[98]

In *Portus Alternative Asset Management Inc. (Re)*,[99] the Ontario Securities Commission successfully applied for an order appointing a receiver of all assets, undertakings and properties of an asset management company. The Court granted the receiver unfettered access to all electronic records for the purpose of allowing the receiver to recover and copy all electronic information, and specifically ordered the debtors not to alter, erase or destroy any records without the receiver's consent. The debtors were ordered to assist the receiver in gaining immediate ac-

97. *Nac Air, LP v. Wasaya Airways Limited*, 2007 CanLII 51168 (ON SC) at para 26.

98. In the decision *Velsoft Training Materials Inc. v Global Courseware Inc.*, 2011 NSSC 274, the Anton Piller order was set aside on the grounds that the discovery that one employee had his computer erased was not sufficient basis to find grave risk that the defendants would destroy evidence.

99. (2005), 28 OSC Bull 2670.

cess to the records, to instruct the receiver on the use of the computer systems and to provide the receiver with any and all access codes, account names and account numbers. In addition, all internet service providers were required to deliver to the receiver all documents, including server files, archived files, recorded messages and e-mail correspondence.

Comment 3.h. All Data Does Not Need to be "Frozen"

Even though it may be technically possible to capture vast amounts of data during preservation efforts, this usually can be done only with significant disruption to IT operations. If a party's established and reasonable practice results in a loss or deletion of some ESI, it should be permitted to continue such practice after the commencement of litigation, as long as such practice does not result in the overwriting of ESI relevant to the case that is not preserved elsewhere.

Imposing an absolute requirement to preserve all ESI could require shutting down computer systems and making copies of data on each fixed disk drive, as well as other media that are normally used by the system—a procedure which could paralyze the party's ability to conduct ongoing business. A party's preservation obligation should therefore not require freezing of all ESI, but rather the appropriate subset of ESI that is relevant to the issues in the action.[100]

Comment 3.i. Disaster Recovery Backup Media

Some organizations have short-term disaster recovery backup media that they create in the ordinary course of business. The purpose of this media is to have a backup of active computer files in case there is a system failure or a disaster such

100. See *Schatz*, *supra* note 80; and *Janzen*, *supra* note 55.

as a fire. Their contents are, by definition, duplicative of the contents of active computer systems at a specific point in time.

Generally, parties should not be required to preserve these short-term disaster backup media, provided that the appropriate contents of the active system are preserved. Further, because backup media generally are not retained for substantial periods, but are instead periodically overwritten when new backups are made, preserving backup media would require a party to purchase new backup media.

In some organizations, the concepts of "backup" and "archive" are not clearly separated, and backup media are retained for a relatively long period of time. Backup media may also be retained for long periods of time out of concern for compliance with record retention laws. Organizations that use backup media for archival purposes should be aware that this practice is likely to cause substantially higher costs for evidence preservation and production in connection with litigation.[101] Organizations seeking to preserve data for business purposes or litigation should, if possible, consider employing means other than traditional disaster recovery backup media.

---

101. See *Farris v. Staubach Ontario Inc.*, 2006 CanLII 19456 at para 19 (ONSC): "In his testimony before me Mr. Straw corrected one statement in the June 28, 2005 letter to the solicitors for the plaintiff. In that letter the solicitors for TSC reported that TSC did not have a separate archival copy of its electronic databases for the November-December 2003 time period. This is not strictly accurate. Sometime in 2004 and probably after June 28, 2004, Mr. Straw had a backup set of tapes made of all information on the TSC server. These tapes have been preserved. While they are not an archival copy of the TSC database for November–December 2003, some of the information on these tapes goes back to that time period. Mr. Straw did not know how many documents were on those preserved archival tapes. However he said they contain in excess of one terabyte of information."

If a party maintains archival data on tape or other offline media[102] not accessible to end users of computer systems, steps should be taken promptly after the duty to preserve arises to preserve those archival media that are reasonably likely to contain relevant information not present as active data on the party's systems.[103] These steps may include notifying persons responsible for managing archival systems to retain tapes or other media as appropriate.[104]

> *Illustration i.* Pursuant to an information technology management plan, once each day a company routinely copies all electronic information on its systems and retains, for a period of 5 days, the resulting backup tapes for the purpose of reconstruction in the event of an accidental erasure, disaster or system malfunction. A requesting party seeks an order requiring the company to preserve, and to cease reuse of, all existing backup tapes pending discovery in the case. Complying with the requested order would impose large expenses and burdens on the company, and no credible evidence is shown establishing the likelihood that, absent the requested order, the producing party will not produce all relevant information during

---

102. Offline data sources refer to those sources of data that are no longer active in the sense that they cannot be readily accessed by a user on the active computer system. Examples of offline data sources include backup tapes, floppy diskettes, CDs, DVDs, portable hard drives, ROM-drive devices, etc.

103. *Mansfield v. Ottawa*, 2012 ONSC 5208 (CanLII) at para 43.

104. Martin Felsky & Peg Duncan, *Making and Responding to Electronic Discovery Requests*, *LawPRO Magazine* (September 2005), online: <http://www.lawpro.ca/LawPRO/ElectronicDiscoveryRequests.pdf>.

> discovery.[105] The company should be permitted to continue the routine recycling of backup tapes in light of the expense, burden and potential complexity of restoration and search of the backup tapes.
>
> *Illustration ii.* An employee was dismissed for cause from a company. Three months later, the former employee sues for wrongful dismissal. During the search for information relevant to the matter, counsel learns that the IT department routinely deletes user inbox e-mails older than 30 days in an effort to control the volume of e-mail on their mail servers. The tape from the last backup of the month is kept for a year before being returned to the backup tape recycling pool. As part of the preservation plan, the backup tapes that are three months and older are retrieved and safeguarded; counsel reasons that tapes used in the daily pool need not be preserved since the evidence they are seeking is at least 90 days old. This is a reasonable position to take. The backup taken just after the employee left is restored and e-mails advancing the employer's case and damaging the plaintiff 's are found.

Finally, if it is unclear whether there are unique, relevant data contained on backup media, the parties or the Court may consider the use of sampling to better understand the data at

105. See *Apotex Inc. v. Merck & Co. Inc.*, 2004 FC 1038 (CanLII) at para 14: "It is clear that the burden of showing that Merck's production is inadequate lies on Apotex, who made that allegation. Apotex must show that documents exist, that they are in the possession or control of Merck and that the documents are relevant."

issue. Sampling will help establish the degree to which potentially relevant information exists on the tapes in question and the likely cost of the retrieval of such information. Consequently, sampling may lead to the informed retention of some, but not all, of the backup media.

> *Illustration iii.* In the course of a search for relevant e-mails belonging to a custodian who left the company's employ a number of years ago, the company discovers that IT has kept the last e-mail backup tape of the week for the past ten years. The backup tapes carry labels with the date of the backup and the server name; however, IT does not have a record of which accounts were stored on which servers. The events happened over a six-month period and the party determines that if there were e-mails, they should most likely appear in the middle of the period. Therefore, it would be reasonable for the company to sample the backup tapes that were labeled with the date in the middle of the range. If a backup of a particular server did not contain e-mails of the custodian, the backups for that particular server could be excluded from further searches.

Comment 3.j. Preservation of Shared Data

A party's networks or intranet may contain shared areas (such as public folders, discussion databases and shared network folders) that are not regarded as belonging to any specific

employee. Such areas should be identified promptly and appropriate steps taken to preserve shared data that is potentially relevant.[106]

> *Illustration i.* Responding to a litigation hold notice from in-house counsel, custodian X identifies the following sources of data relevant to an engineering dispute that she has in her possession or control: e-mail, word-processing and spreadsheet files on her workstation and on the engineering department's shared network drive, as well as a collection of CD-ROMs with relevant data and drawings. Following up on her response, counsel determines that custodian X also consults engineering department knowledge management databases, contributes to company wikis and discussion groups and is involved in online collaborative projects relevant to the dispute. Although custodian X does not consider herself to be in possession or control of these additional sources, counsel should work with the IT department to include these in the preservation process.

Principle 4. Counsel and parties should cooperate in developing a joint discovery plan to address all aspects of discovery and should continue to cooperate throughout the discovery process, including the identification, preservation, collection,

106. *Drywall Acoustic, supra* note 85 at paras 111–112.

processing, review and production of electronically stored information.

Comment 4.a. The Purpose of Discovery Planning

The purpose of discovery planning[107] is to identify and resolve discovery-related issues in a timely fashion and to make access to justice more feasible and affordable. The process is not intended to create side litigation.[108] Cooperation includes collaboration in developing and implementing a discovery plan to address the various steps in the discovery process. These will include some or all of the following steps: the identification,

107. It has been common to refer to the "meet-and-confer" process, or to say that the parties will "meet-and-confer" or attend a specific "meet-and-confer" session. While this Commentary will still use this term, the point is not that there must be one or more meetings; the emphasis should be on conferring with a view to reaching meaningful agreement on a discovery plan.

108. *Drywall Acoustic*, *supra* note 85 at paras 81–84.

preservation, collection and processing of documents;[109] the review and production of documents;[110] how privileged documents are to be handled or other grounds to withhold evidence; costs; and protocols.

While the original *Principles* primarily discussed the "meet-and-confer" process, the Canadian collaborative experience has developed more significantly around the principle of ongoing cooperation and the development of a discovery plan. The idea of cooperation between counsel and parties extends well beyond the confines of a meeting, or series of meetings, to transparent sharing of information in an effort to keep discovery costs proportionate and timelines reasonable. Accordingly, based on the universal consensus of the participants in The Sedona Conference Working Group 7 August 2014 Meeting in Toronto, the language in these *Principles* has moved towards "cooperation" and "collaboration" in lieu of the more restrictive "meet-and-confer" term.

---

109. "Processing" means "an automated computer workflow where native data is ingested by any number of software programs designed to extract text and selected metadata and then normalize the data for packaging into a format for the eventual loading into a review platform. [It] [m]ay also entail identification of duplicates/de-duplication." The Sedona Conference, *Glossary: E-Discovery & Digital Information Management* (April 2014), *supra* note 9. Processing can also involve steps to deal with documents that require special treatment, such as encrypted or password-protected files. Parties should avoid making processing decisions that have consequences for others without first discussing those decisions. An effective discovery plan will address issues such as the means of creating hash values, whether to separate attachments from e-mails and which time zone to use when standardizing DateTime values.

110. Parties may consider adopting a staged or phased approach to e-discovery where appropriate due to the volume of evidence. Parties should also agree as early as possible on production specifications.

A successful discovery plan will ensure that the parties emerge with a realistic understanding of what lies ahead in the discovery process. To address the increasing volumes of ESI and the high costs of litigation, these *Principles* strongly encourage a collaborative approach to e-discovery, reflecting recent judicial opinions and attitudes in Canada and other countries.[111] "Common sense and proportionality" have been described as the driving factors of discovery planning.[112]

In Ontario, the *Rules of Civil Procedure* were amended in 2010 to require the parties "to agree to a discovery plan in accordance with [Rule 29.1]."[113] The development of a meaningful

111. *Wilson v. Servier Canada Inc.*, 2002 CanLII 3615 (ON SC) [*Servier*] at paras 8–9: "The plaintiff's task in seeking meaningful production has been made particularly difficult by the defendants' general approach to the litigation. On the simple premise, as expressed by the defendants' lead counsel, that litigation is an adversarial process, the defendants have been generally uncooperative and have required the plaintiff to proceed by motion at virtually every stage of the proceeding to achieve any progress in moving the case forward. I take exception to this. In contrast with other features of the civil litigation process in Ontario, the discovery of documents operates through a unilateral obligation on the part of each party to disclose all relevant documents that are not subject to privilege. The avowed approach of the defendants' counsel is contrary to the very spirit of this important stage of the litigation process." See also *Sycor Technologies v. Kiaer,* 2005 CanLII 46736 (ON SC). In dispute was the form of production in a case where just the cost of printing e-mails was going to be $50,000 or so. The Court indicated that "procedural collaboration and a healthy dose of pragmatism and common sense" were required, and sent counsel back to work out an efficient method of production in accordance with the Ontario Guidelines.

112. *Drywall Acoustic*, *supra* note 85 at para 84.

113. *Rules of Civil Procedure*, RRO 1990, Reg 194, r 29.1.03(3) states that the plan shall include:

discovery plan requires meaningful and good-faith collaboration and information sharing between the parties that is proportionate and relevant to the nature of the individual action. Additionally, there is an ongoing duty to update the discovery plan as required.

In Quebec, the modifications to the *CCP* introduced the notion of cooperation by requiring the parties to agree on the conduct of the proceeding before the presentation of the introductory motion. A new chapter regarding case management was added to the *CCP* to ensure that parties take control of their case in accordance with the new section 4.1 *CCP*.[114]

To be effective, the discovery plan must be a "meeting of the minds" regarding the discovery process. The end result should be to reach agreement on a written discovery plan. This

---

> a) the intended scope of documentary discovery under rule 30.02, taking into account relevance, costs and the importance and complexity of the issues in the particular action;
>
> b) dates for the service of each party's affidavit of documents (Form 30A or 30B) under rule 30.03;
>
> c) information respecting the timing, costs and manner of the production of documents by the parties and any other persons;
>
> d) the names of persons intended to be produced for oral examination for discovery under rule 31 and information respecting the timing and length of the examinations; and
>
> e) any other information intended to result in the expeditious and cost-effective completion of the discovery process in a manner that is proportionate to the importance and complexity of the action.

114. CQLR c C-25, s 151.1–151.23.

is a best practice whether or not such a plan is prescribed by the rules of court of the applicable jurisdiction.[115]

The planning process may vary greatly, depending upon the scope and nature of the action. For example, a modest straightforward action may require a discovery plan that consists of a few paragraphs developed via telephone call or e-mail exchanges between counsel. A more complex case may require a series of in-person meetings and a more comprehensive plan.[116] Counsel should decide in each individual case what sort of meeting and discovery plan will be appropriate. Factors to be considered will include, but not be limited to: the amount at stake in the action, the volume and complexity of the electronic evidence to be exchanged, the location of counsel and other issues relevant to the discovery process.

An Ontario Court has held that "[t]he interplay between the *Rules of Civil Procedure*, Rules of Professional Conduct, Principles of Civility and Professionalism and the relatively new requirement for formal discovery planning is important."[117] The Courts have criticized counsel for failing to create a discovery plan, and have in some cases sanctioned counsel conduct using cost rules.[118]

---

115. For a sample discovery agreement and other model documents, see OBA, Model Precedents, *supra* note 70.

116. *Enbridge Pipelines Inc. v. BP Canada Energy Company*, 2010 ONSC 3796 at paras 3–4 (CanLII) (C. Campbell J.). The Court endorsed a discovery plan in a complex piece of litigation, but emphasized that not every case would require this level of detail.

117. *Kariouk v. Pombo*, 2012 ONSC 939 (CanLII) [*Kariouk*] at para 3, see also paras 55–56.

118. *Corbett v. Corbett*, 2011 ONSC 7161 (CanLII) [*Corbett*]; *Petrasovic Estate v. 1496348 Ontario Ltd.*, 2012 ONSC 4897 (CanLII) [*Petrasovic*]; *Siemens*,

Comment 4.b. Confer Early and Often

Parties should confer early in the litigation process and thereafter as appropriate. The first contact should take place as soon as possible after litigation has commenced and in any event prior to the collection stage. The parties should, at a minimum, confer as soon as the pleadings have closed to ensure the scope of the required collection is known.

While parties may have taken many, if not all, of the steps necessary to preserve potentially relevant information by the time they confer, there may be additional preservation issues for discussion. For example, if additional custodians are added to the list, or if timelines are agreed upon that are broader than originally anticipated by the parties, additional preservation steps will be required.

Meeting early is one of the keys to effective e-discovery. Decisions made about e-discovery from the earliest moment that litigation is contemplated will have serious impact on the conduct of the matter, not to mention the potential cost of discovery. Opening up discussion and debate on ESI early in the process avoids subsequent disputes, which may be costly and time consuming.

> *Illustration i*. A manufacturer defending a product liability claim issues a litigation hold to the operations division, captures the hard drives and server e-mail of twelve production managers and uses a long list of search terms drafted by in-house counsel to cull the data. Outside counsel spend six months reviewing the data before it is produced, almost a year after the litigation was launched.

---

supra note 46; 1414614 *Ontario Inc. v. International Clothiers Inc.*, 2013 ONSC 4821 (CanLII) [*International Clothiers*].

> The receiving party now argues that (a) all data from the marketing department relating to the defective product should also have been preserved; (b) there are eight additional managers, four of whom have since left the company, whose e-mails should have been preserved and reviewed; (c) the list of search terms is demonstrably too narrow according to its e-discovery expert; and (d) backup media containing highly probative evidence should have been restored because active end-user e-mail stores are purged every 90 days in accordance with the company's records management policy. If the parties had met at the beginning of the process many of these issues could have been addressed and dealt with in the discovery plan.

A single meeting will not be sufficient for the development of an appropriate discovery plan in some cases. Accordingly, Principle 4 envisions not just a single meeting but an ongoing series of discussions.[119] Those ongoing discussions assist counsel when they encounter unanticipated technical issues. In

119. See e.g. *L'Abbé, supra* note 51 at para 31, in which the Master held: "First and foremost, when dealing with vast numbers of documents, particularly electronically stored information, the parties ought to be devising methods for cost effectively isolating the key relevant documents and determining claims of privilege. To the extent that there is disagreement about the scope of relevance or privilege, it may be necessary to obtain rulings from the court but the onus is on counsel to jointly develop a workable discovery plan and to engage in ongoing dialogue." See also *Kaymar v. Champlain CCAC*, 2013 ONSC 1754 (CanLII) at para 37 (M. MacLeod) [*Kaymar*], in which the Master stated his view that discovery plans should be flexible. "In a perfect world, the discovery plan would be a living breathing process, modified, adapted and updated as necessary."

some situations, the volume of data to be collected and reviewed is underestimated, and search criteria used to cull the collection may need to be reviewed and adjusted if results are not sufficiently precise or relevant. These developments should be communicated to all parties. Absent such communication, any agreement reached through initial cooperation can easily evaporate.

As one Court has stated, "[t]he obligation to engage in discovery planning includes an obligation to confer at the outset and to continue to collaborate on an ongoing basis in order that the plan may be adjusted as necessary."[120] This obligation does not disappear because there is an order of the Court regarding discovery.[121]

Comment 4.c. Preparation for Planning

Counsel should participate in the planning process in good faith and come prepared to discuss several key issues in a substantive way. Those issues include identifying the sources of potentially relevant ESI, the steps to be taken for preservation and the methodology to be used to define and narrow the scope of the data to be reviewed and produced.

Depending on the nature of the discovery project and the scope of the litigation, preparation should also include collecting information from knowledgeable people within the client organization. These people may include a business manager or managers familiar with the operational or project areas involved in the litigation and the key players in the organization, someone familiar with the organization's document and records

120. *Kariouk, supra* note 117 at para 42.

121. *International Clothiers*, *supra* note 118 at para 20.

management protocols and the IT manager or managers familiar with the organization's network, e-mail, communication and backup systems. These individuals may also attend the discovery plan meeting(s) where appropriate. (See Comment 4.d. below).

Ideally, a written agenda should be prepared that sets out the key issues for discussion for the development of the discovery plan. Topics for the discovery plan meeting agenda will commonly include:

Comment 4.c.i. Identification

To prepare for the discovery plan meeting in a meaningful way, counsel should consult with IT staff, outside service providers, users and others to gain a thorough understanding of how ESI is created, used and maintained by or for the client, and to identify the likely sources of potentially relevant ESI.[122]

Comment 4.c.ii. Preservation

In developing the discovery plan, parties should discuss what ESI falls within the scope of the litigation and the appropriate steps required to preserve what is potentially relevant. If unable to reach a consensus the parties should apply on an ur-

122. See *Canada (Commissioner of Competition) v. Air Canada (TD)*, [2001] 1 FC 219 at para 27, 2000 CanLII 17157 (FCTD): "Counsel for the Commissioner noted that, at the time the Commissioner sought the section 11 order, he did not know what the record-keeping practices of Air Canada were. Counsel indicated that insofar as there were real difficulties in responding to the requests, as a result of the form in which they had been asked, this should be the subject of discussion between counsel, before the Court was asked to adjudicate further on it. That aspect of Air Canada's present motion was therefore set aside to allow for such discussion."

gent basis for court direction, or at the very latest after the delivery of pleadings, to ensure that relevant information is not destroyed.

While making copies of hard drives is useful in selective cases for the preservation phase, the processing of the contents of the hard drives should not be required unless the nature of the matter warrants the cost and burden.[123] Making forensic image backups of computers is often not required and should be discussed. Engaging in this process can divert litigation into side issues involving the interpretation of ambiguous forensic evidence. The key is for counsel to agree on reasonable, proportionate steps to ensure potentially relevant information is available for production.

Comment 4.c.iii. Collection and Processing

The parties should also discuss the steps they will take to narrow the potentially relevant information to a smaller set that is reasonable and proportionate in the context of the lawsuit. Typical selection criteria used to narrow the scope of the ESI include the names of key players, timelines, key data types, key systems (e.g. accounting), de-duplication and search terms. Every effort should be made to discuss and agree on these issues.

---

123. *Janzen*, *supra* note 55 at para 1: "This is an application to compel the defendant to produce a Supplemental List of Documents, listing his hard disk drives (HDD) and a mirror image copy of those hard disk drives as documents in its possession. The plaintiff wants the mirror-image HDD produced to its own computer expert for a computer forensic analysis;" and at para 36: "Without some indication that the application of the interesting technology might result in relevant and previously undisclosed documents, the privacy interests of the third parties and the avoidance of unnecessary and onerous expense militate against allowing such a search merely because it can be done."

Parties and counsel should agree on (1) the use of selection criteria as a means to extract targeted, high-value data; (2) the type(s) and form(s) of selection criteria to be used; (3) a process for applying the agreed-upon selection criteria; (4) specific search terms that will be used; and (5) a protocol for sharing and possibly adjusting the criteria. Absent such agreement, parties should be prepared to disclose the parameters of the search criteria that they have undertaken and to outline the scope of what they are producing and what sources or documents have not been searched.

Comment 4.c.iv. Review Process

Issues for discussion in connection with the review stage will include: the scope of the review; whether it will be conducted manually or with the assistance of electronic tools such as concept-clustering or predictive coding technologies; and the methods to be used to protect privileged, personal and confidential information and/or trade secrets. For more information, The Sedona Conference has published a Commentary on search and retrieval methods and technologies.[124]

Comment 4.c.v. Production

Counsel should discuss the form in which productions will be exchanged—for example, whether certain document types will be in native format (commonly used for PowerPoint presentations and Excel spreadsheets) or static images. Counsel would benefit from a detailed discussion even where source documents are in paper form, or where, as is commonly the

124. The Sedona Conference, *Best Practices Commentary on the Use of Search and Retrieval Methods in E-Discovery* (2013), 8 Sed. Conf. J. 189, online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/3669>.

case, source documents exist in both hard copy and digital format.[125] Early agreement on production specifications can save significant time and expense later in the process. Involving service providers in these discussions early in the process can help to avoid delays, mistakes and re-work.

Comment 4.c.vi. Timing

Counsel should discuss the schedule and timing for the processing, review and production of ESI and should also address the need for additional discussions throughout the matter and a resolution process for any issues that may arise.[126] [127]

125. *Logan v. Harper*, 2003 CanLII 15592 (ONSC) [*Logan*] at para 66: "Before indexing and scanning the documents, it would be useful for the parties to discuss how the documents are to be identified and organized and to agree upon the electronic format for the documents. If the parties can agree on a mutually acceptable system it may well save time, cost and confusion. It may be that Health Canada has an indexing and identification system that it would be appropriate to adopt."

126. See *Kaymar, supra* note 119 at paras 37–38 (M. MacLeod), in which the Master expressed his preference that discovery plans contain a "sophisticated non adversarial process" for dispute resolution. Although acknowledging the central role of courts in adjudicating disputes and supervising the discovery phase of cases, he stated: "A well-crafted plan should minimize the need for court intervention and utilize adversarial adjudication as a last resort. A contested motion with court inspection of disputed documents is inherently a cumbersome and expensive way to resolve discovery disputes."

127. In *2038724 Ontario Ltd. v. Quiznos Canada Restaurant Corp*., 2012 ONSC 6549 (CanLII) (Justice Perell) at paras 129-130 [*Quiznos*], the Court ordered a party to reproduce documents in Excel format despite the fact that the discovery plan had agreed that productions would be exchanged in TIFF. The Court found that there would be no hardship or difficulty in providing the documents in native format; and, that while important, discovery plans can be modified.

The preservation, collection, processing, review and production steps are considered in greater detail in Principles 3, 5, 6, 7 and 8.

Comment 4.d. Who Should Participate

In the e-discovery context, the development of a discovery plan is like any business planning meeting: if the right people are at the table, the agenda is set out in advance, the participants are prepared and the decisions are recorded and followed up upon, then the meeting will have a greater likelihood of success. Multi-party and class actions in particular need to have involvement from different points of view. Even if no in-person meetings take place, the same principles apply: clear objectives, good record-keeping, open communication and meaningful follow-up.

In many cases, each party involved in discovery planning may benefit from the participation of an e-discovery advisor with experience in the technical aspects of discovery, especially where complex technology, legacy systems or database information may be issues.

Principle 4 suggests that counsel and parties should both be involved, since matters to be addressed are not limited to legal issues alone. Although discovery planning should take place within the context of substantive and procedural law, important considerations may arise that are almost certain to be beyond the range of counsel's expertise. This is not a task to be delegated to junior lawyers. Given the nature and implications of a discovery plan, it is valuable to have senior counsel involved in these discussions.

In many cases, clients should also participate. The client will be able to state upfront what information is available, and in what format. Further, having the client involved increases the

openness of the process. The person who has best knowledge of the relevant data sources and systems should be present or at least consulted before the parties agree to a discovery plan.

In cases involving financial loss or evidence, the courts have suggested that the accountants participate in the planning process so that the disclosure could be targeted to what was actually needed by the parties to prove their case.[128]

Comment 4.e. Good-Faith Information Sharing to Facilitate Agreement

As stated above, an effective discovery planning process requires a meeting of the minds. The purpose is to facilitate proportionate discovery, not to create roadblocks. Open and good-faith sharing of relevant information is required for this purpose.

Discovery planning discussions are generally held on a "without prejudice" basis to facilitate the required level of openness. Once the discovery plan is signed, it becomes a "with prejudice" agreement.

The types of information properly exchanged during discovery planning are not privileged. These types of information include: search terms,[129] names of custodians, systems from which information will be retrieved and the e-discovery process developed by the parties for use in the case. Further, describing discovery processes does not disclose trial strategy or limit counsel from being strong advocates for their clients' interests. Instead, it ensures a defensible framework inside which the case can proceed. Once the discovery plan is agreed upon, counsel

128. *International Clothiers Inc., supra* note 118.

129. If search terms include terms that may be considered trade secrets, only then would they be excluded, on grounds of confidentiality.

can focus on the substantive aspects of and strategies for their case.

Accordingly, parties should describe the methodology they are employing for their case, including any steps they are taking to validate their results. If objections are raised to the validity or defensibility of the proposed process, the objections should be dealt with at the earliest possible stage. This level of openness ensures the discovery plan is meaningful and defensible at the earliest possible stage, potentially saving the clients the time, money and aggravation of having to re-do discovery processes at a much later date.

In cases where the parties (or a party) resist sharing relevant information or refuse to engage in the discovery planning process at all, counsel may consider sending a draft discovery plan to opposing counsel with a time line for agreement on its terms. If no response is received, the draft discovery plan may form the subject matter of a motion for court approval.[130]

Comment 4.f. Consequences of Failing to Cooperate

The courts have criticized counsel for failing to meet their obligations, referring to the "interplay between the Rules of Civil Procedure, Rules of Professional Conduct, Principles of Civility and Professionalism and the relatively new requirement for formal discovery planning."[131]

While the courts have confirmed a party may apply to the courts for a discovery plan when agreement cannot be reached, this is not intended to allow counsel to abdicate their

130. Courts have exercised their ability to impose discovery plans. See e.g. *Ravenda v. 1372708 Ontario Inc.,* 2010 ONSC 4559 (CanLII), and *TELUS Communications Company v. Sharp,* 2010 ONSC 2878 (CanLII).

131. *Kariouk, supra* note 117 at para 3.

responsibility to cooperate and draft a plan.[132] A risk all parties face when reliant on the courts for a discovery plan is that they lose control over the decision-making process and the courts may not be in a better position to determine the most appropriate plan.[133]

The parties continue to have an ongoing obligation to confer and make adjustments and disclosures where necessary.[134] Adverse cost consequences are a serious risk in discovery motions for parties who fail to act reasonably or fail to meet their obligations.[135] In Nova Scotia, the failure to come to an agreement on electronic disclosure results in the default provisions of Civil Procedure Rule 16, which include an obligation to perform all reasonable searches, including keyword searches, to find relevant electronic information.[136]

Principle 5. The parties should be prepared to produce relevant electronically stored information that is reasonably accessible in terms of cost and burden.

Comment 5.a. Scope of Search for Reasonably Accessible Electronically Stored Information

The primary sources of ESI in discovery should be those that are reasonably accessible. Typically this includes e-mails and electronic files (such as Word, PowerPoint and Excel documents) that can be accessed in the normal course of business.

132. See *Siemens, supra* note 46 at paras 79–84.

133. *Siemens, supra* note 46.

134. *International Clothiers Inc., supra* note 118; *Siemens, supra* note 46.

135. *Corbett, supra* note 118; *Petrasovic, supra* note 118; *Siemens, supra* note 46.

136. *Velsoft, supra* note 14.

Parties should be prepared to produce relevant ESI that is "reasonably accessible" in terms of cost and burden.

Whether ESI is "reasonably accessible" requires an assessment of the following issue: will the quantity, uniqueness or quality of data from any particular type or source of ESI justify the cost of the acquisition of that data? Essentially, it is a cost-benefit analysis. Certain forms of ESI—such as old backup tapes, data for which applications no longer exist, information that was available on old web pages and information in databases—are often assumed to be "not reasonably accessible" simply because they are more difficult to deal with than other data forms. This is not always the case.

To enable the Court to perform that cost-benefit analysis, counsel will be required to provide clear information on the types of media that will need to be searched (e.g. backup tapes, microfiche, etc.), the status of the media and its condition (e.g. media that is in a damaged state, media stored in boxes, etc.) and the likelihood of retrieving data from the media in a useable form. The Court may require expert evidence on all of the above points as well as the costs associated with the retrieval of the data and the time required for the data retrieval. It is not sufficient for the party resisting production to simply argue that it is expensive.

Recent cases show that Canadian courts have been aware of the need for this cost-benefit analysis. For example, in *Murphy et al v. Bank of Nova Scotia et al*,[137] the Court considered the plaintiff's request that additional e-mail information contained in backup tapes be produced by the defendant bank for a period of almost three years. The defendant argued this would cost be-

137. 2013 NBQB 316 (CanLII).

tween $1.2 million (for 13 employees) and $3 million (for 33 employees). The Court noted that ". . . the burden, cost, and delay of the production must be balanced against the probability of yielding unique information that is valuable to the determination of the issues. Counsel for the plaintiffs made reference to a possible 'smoking gun' that could exist in one of the many e-mails authored by [the bank's] employees. This is way too speculative." In the end, the Court ordered that the e-mails from only four employees be retrieved for a period of just over one month.

In *Hudson v. ATC Aviation Technical Consultants*,[138] the Master ordered the appellants—manufacturers of an airline engine identified as one of the causes of a fatal airline crash—to produce 39 years of documents concerning 15 parts and over 50 models, some of which were not even at issue in the lawsuit. The appellants appealed on the ground that the request was disproportionate and excessive. The Court held that the documents were relevant, not just to show that the defendants had a propensity to manufacture improperly, but to show that they knew of issues with similar systems that were probative of what it knew, did and said in relation to the engine and accident in this case. The appellants filed no evidence as to how accessible the data was. The Court held that absent evidence from the appellants demonstrating the hardship incurred in producing the records sufficient to counterbalance the relevancy and discretionary factors, the production order would stand.

Where the Court determines that the efforts to obtain the data do not justify the burden, it will exercise its discretion to

138. *ATC Aviation*, *supra* note 69.

refrain from ordering production of relevant documents. For example, in *Park v. Mullin*,[139] the Court noted that in the past it has "used its discretion to deny an application for the production of documents in the following circumstances: (1) where thousands of documents of only possible relevance are in question . . .; and (2) where the documents sought do not have significant probative value and the value of production is outweighed by competing interests, such as confidentiality and time and expense required for the party to produce the documents. . . ."

Owing to the volume and technical challenges associated with the discovery of ESI, the parties should engage in the above cost-benefit analysis in every case—weighing the cost of identifying and collecting the information from each potential source against the likelihood that the source will yield unique, necessary and relevant information. The more costly and burdensome the effort to access ESI from a particular source, the more certain the parties need to be that the source will yield relevant information. However, the fact that an organization does not proactively manage its information or has poor information governance practices should not itself operate in support of any argument that it should not be compelled to produce due to undue burden or cost in complying with its discovery obligations.[140]

A production request pertaining to an ESI source that is determined to be "not reasonably accessible" must be justified by showing that the need for that particular data outweighs the

139. 2005 BCSC 1813 (CanLII).

140. See e.g. Master Short's decision in *Siemens*, *supra* note 46 at paras 136–138, and 156, where he states that Sapient's e-mail retention policy which deletes e-mails after 30 days can cause serious problems, and ordered Sapient to restore and search backup tapes, despite counsel's argument that such an Order would be disproportionately costly.

costs involved.[141] Information that is otherwise relevant may be excluded on the grounds that recovery of that information involves an inordinate amount of time or resources which are not commensurate with the potential evidentiary value.[142]

Parties and courts should exercise judgment based on reasonable good-faith inquiry, taking into consideration the cost of recovery or preservation. If potentially marginally relevant documents are demanded from sources for which the information is difficult, time-consuming or expensive to retrieve, cost shifting may be appropriate.

In some jurisdictions, particularly where case management is available, a party may apply for directions regarding its discovery obligations. Seeking advance guidance may avoid a contentious after-the-fact dispute where the onus may lie on the producing party to demonstrate why it did not initially produce the requested information.

> *Illustration i.* In an employment case, the plaintiff employee claims to have received abusive e-mail from his supervisor as part of an ongoing pattern of harassment. The employee claims that the e-mail would have been sent 18 months ago. There are no backup tapes from the period and the plaintiff did not keep any copies. The employer company has imaged the workstation and conducted a thorough search of all e-mail folders, including

141. *Descartes v. Trademerit*, 2012 ONSC 5283 (CanLII); *GasTOPS Ltd. v. Forsyth*, [2009] OJ No 3969 (CanLII).

142. *R. v. Mohan*, [1994] 2 SCR 9, as quoted in *Gould Estate v. Edmonds Landscape & Construction Services Ltd.*, 1998 CanLII 5136 (NSSC), 166 NSR (2d) 334.

the deleted items folder, but the e-mail was not located. The plaintiff asks the Court to order a forensic examination of the computer to recover the deleted information. In the absence of any evidence from the plaintiff as to the existence of the abusive e-mail, the Court accepts the defendant's argument that the probability of finding traces of an e-mail that was deleted 18 months ago from a workstation that is in daily active use is negligible as the space on the disk would have been overwritten in the normal course of business.

Illustration ii. An unsuccessful bidder on a municipal government's request for proposals (RFPs) for a multi-million dollar construction contract alleges unfairness and impropriety. The final report of the evaluation committee was in printed format. The plaintiff alleges that the criteria used to compare the bids were changed during the evaluation. The plaintiff asks for the electronic version of the selection criteria that, according to the municipal government's RFP policy, must be determined before the RFP is released. The plaintiff explains that this document is material and necessary to its prosecution of the case. It has, however, been three years since the competitive tender, and due to staff turnover, the electronic version has been lost. However, a backup copy on the server used by the former contracts officer is available and can be recovered. Since the backup copy would be the only source for a piece of critical information in the suit, the Court orders the recovery of the electronic version from the server.

Comment 5.b. Outsourcing Vendors and Other Third-Party Custodians of Data

Many organizations outsource all or part of their information technology systems or share ESI with third parties for processing, transmitting or for other business purposes. Cloud storage is one example of this type of arrangement. In contracting for such services, organizations should consider how they will comply with their obligations to preserve and collect ESI for litigation. If such activities are not within the scope of contractual agreements, costs may escalate and necessary services may be unavailable when needed. Parties to actual or contemplated litigation may also need to consider whether preservation notices should be sent to non-parties, such as contractors or vendors.

Principle 6. A party should not be required, absent agreement or a court order based on demonstrated need and relevance, to search for or collect deleted or residual electronically stored information that has been deleted in the ordinary course of business or within the framework of a reasonable information governance structure.

If ESI has been deleted in the ordinary course of business or within the framework of a reasonable, defensible information governance structure and is no longer easily accessible, then a party should not be required, absent agreement or a court order based on demonstrated need and relevance, to search for or collect deleted or residual ESI. The need to identify, preserve and collect this type of data will be rare. While deleted or residual ESI may be required in any case, it is more likely to be relevant in criminal cases or those involving fraud.

As noted above, it is important to note that just because data has been deleted does not automatically mean that the data is difficult to access. Further investigations need to be made to validate that determination. For example, in some cases files that have been deleted remain readily retrievable from a party's computer system without any special expertise. In those cases, the courts are more likely to order production.[143]

Whether a court will order the production of deleted or residual ESI that is not easily accessible is a case-by-case determination. Courts will consider a number of factors including,

143. See *Low, supra* note 55 where the Court refused to order a forensic analysis of the plaintiff's hard drive for files that may have been deleted because of the significant costs and limited probative value of the files requested. The Court did, however, order that the plaintiff search for relevant files that had been deleted but which were still readily retrievable by using the computer's operating system.

but not limited to, the principle of proportionality, proof of intentional destruction of data and the scope of the search.

In *Holland v. Marshall*,[144] the plaintiff's hospital records had been destroyed. However, at the time the records were destroyed, the hospital had a policy in place to destroy adult records after the lapse of 11 years. The Court found that before the plaintiff's records were destroyed, litigation was not threatened nor reasonably apprehended by the hospital or any of the other defendants.

In *Patzer v. Hastings Entertainment Inc.*,[145] the plaintiff had deposited a number of betting slips into an automated gaming machine at the Hastings Park Racecourse in Vancouver. The plaintiff received from the machine a cash voucher in the amount of $6.5 million. The defendant refused to honour the voucher on the grounds that it was issued in error. The plaintiff sought production of a number of documents, including the betting slips. The standard practice at Hastings Park was that the betting slips were purged from each automatic machine on a weekly or bi-weekly basis and then sent out for recycling. When the documents were destroyed there was no evidence that the plaintiff was contemplating litigation. The Court held that the documents were destroyed in the ordinary course of business and there was no basis to apply the doctrine of spoliation.

> *Illustration i.* A plaintiff seeking production of relevant e-mails demands a search for e-mails deleted by the defendant during the normal course of business. The e-mails are not easily accessible. The plaintiff has not provided any justification or evidence that would suggest a particular need for

144. *Holland v. Marshall*, 2008 BCCA 468.

145. *Patzer v. Hastings Entertainment Inc.*, 2011 BCCA 60.

the deleted e-mails. The request would likely be denied by the Court as the production request is not proportionate; parties are not typically required to search the trash bin outside an office building after commencement of litigation.

Illustration ii. A defendant in a lawsuit has an existing information governance structure that set out that e-mails would be kept for 2 years. A lawsuit is brought, and the plaintiff requests e-mails going back 3 years. On a motion, the defendant explained the rationale for its 2 year e-mail retention policy and the costs involved in retrieving older e-mails from backup tapes. The Court holds that the defendant had a reasonable information governance structure and is not required to provide e-mails older than 2 years old.

Principle 7. A party may use electronic tools and processes to satisfy its documentary discovery obligations.

Comment 7.a. Greater Accuracy, Efficiency and Cost Control Through the Effective Use of Technology

Modern e-discovery tools have progressed to the point where virtually every phase of e-discovery can be made more accurate (in terms of the quality of the results), more defensible (in terms of the processes involved), more efficient (in terms of resources), more speedy and even more cost-effective than in the past.[146]

146. It is likely that not all of these benefits can be enjoyed at the same time; the normal trade-offs among speed, resource efficiency, overall cost and quality will still exist. However, there have been many reports of large

Parties who deploy appropriate technology at the right stages of the discovery lifecycle and as part of well-planned and well–managed processes, can in many cases achieve all three of "faster, better, cheaper." In many situations they can expect to spend less time and money than in the recent past while arriving at production sets that contain a higher proportion of the relevant documents that existed in the initial population (higher "recall") while also handing over fewer nonresponsive documents than were traditionally included in productions (higher "precision").[147] These tools also offer the significant benefit of bringing the most important documents to the fore much earlier in the project. The following sections discuss the most important uses of technology to achieve greater accuracy, efficiency and savings.

Comment 7.b. Appropriate Technology Within a Defensible Process

Tools must be chosen with a view to their reliability. Ultimately, the reliability of the entire production process is dependent on both the intelligent application of the appropriate tools and the process put into place. Put another way, it is imperative to develop and implement a defensible process. Any party that relies on technology to assist with the determination of relevance or privilege should ensure that the technology is

---

complex e-discovery projects in which the effective use of appropriate technology has made the process faster, better *and* cheaper than traditional linear review by teams of lawyers. What may seem like an added cost at the start of a project, e.g. for processing or analytics, can be the means of achieving better results and saving even greater amounts—and weeks or months of review time—later in the project.

147. For a full discussion of "recall" and "precision," see *infra*, Comment 7.d.

able to do what it says it can do, and can do so reliably. Parties may need to consult an expert on this issue if appropriate.

Where possible, parties should agree in advance on (1) the scope of data to be searched; (2) the use of de-duplication software to remove "true" duplicate documents; (3) the search tools to be used (e.g. search terms, concept searching, predictive coding); and (4) the method for validating the results. Absent such an agreement, parties should document for the Court the process and methodology used, including decisions to exclude certain types or sources of documents, in the event the approach taken is questioned.

Comment 7.c. Techniques to Reduce Volume

No matter how targeted and selective a party may be in identifying, preserving and collecting data, the majority of the ESI collected is likely to be irrelevant or only marginally relevant. It can therefore be impractical or prohibitively expensive to review all the information. Parties should therefore consider and discuss the use of appropriate technology throughout the discovery process.[148]

As new technologies emerge, parties should assess them and (and with the advice of experts, where appropriate) continue to embrace them. That being said, the most effective way to keep volumes of data as modest as possible is to maintain good, defensible information governance processes.[149]

---

148. Smaller volume collections may also benefit from the application of technology. Providing that the process is efficient and proportionate, there can be a significant return on investment for the use of technology instead of a completely manual review.

149. For discussion of Information Governance, see *supra*, Comment 3.b.

Comment 7.c.i. Data Metrics Report

When dealing with electronic records, a "data metrics" report can be created before data is collected and can be a useful tool to limit the collection of irrelevant documents. It can also be used after data collection (and is also useful for removing irrelevant documents at that point). A data metrics report provides information such as the types of file extensions in the data, the dates of the documents, custodians and file organization. This information can be used to eliminate categories of unnecessary data.

Collecting information and understanding the nature of the data as early as possible is a best practice. There are many new tools that provide highly sophisticated reports that will quickly allow counsel and their technical advisors to understand and assess a collection of information.

> *Illustration*. If photographs are not relevant to a case, the volume of digital photographs within a collection can be ascertained immediately, and a decision can be made to automatically identify and remove these records prior to processing or review.

Comment 7.c.ii. Duplicate Documents

Sources of ESI often include multiple copies of the exact same, or nearly the same, document or e-mail. There are electronic tools available to limit the volume of these types of documents.

a) De-Duplication

De-duplication or "de-duping" refers to a process of identifying exact duplicate[150] e-mails or other computer files and setting aside the copies. Depending on the case, de-duplication can save considerable amounts of time and money. In most cases, it will be appropriate to eliminate exact duplicates.

> *Illustration.* A company with hundreds of employees will have hundreds of copies of a relevant company policy that was e-mailed to each employee. It is not necessary to review hundreds of copies of the same policy, which would greatly increase the cost of the related review. Consider also the situation where a copy of a contract is saved by all employees in the department to their individual hard drives. It is only necessary to review one copy of this contract.

De-duplication can be performed within each custodian's data set or, more commonly, "across" all files ("case-wide de-dupe"). Where it is important to know whether a particular document existed in the files of a particular person, a party would perform custodian-level de-dupe, which ensures that the party will see each document that a person possessed, even if the same document exists in the files of other custodians. If it is

---

150. De-duplication should be limited to those documents or data items that are exactly alike (typically confirmed by comparing the documents' "hash" values). It should be noted that specific elements from a document or data item, such as author, creation date and time, size, full text and the like, can be used alone or in combination to develop targeted de-duplication algorithms. A "hash" is a mathematical algorithm that represents a unique value for a given set of data, similar to a digital fingerprint. Common hash algorithms include MD5 and SHA1. The Sedona Conference, *Glossary: E-Discovery & Digital Information Management* (April 2014), *supra* note 9.

not important to know whether a document existed in each person's files, the review team only needs to see it once in the whole case; here, in such cases, a case-wide de-dupe will be used. Understanding the implications of de-duplication technologies and choices is an important part of discovery planning.

b) Near Duplicates

A process called near-duplicate identification identifies documents that are substantially the same, although they may contain minor differences. For example, if a party has a business report generated on a weekly basis, these records will be similar but not identical to each other.

By grouping highly similar documents together, near-duplicate identification helps to expedite the review. This efficiency will save considerable time and cost and increase the quality and accuracy of the review.

c) E-mail Threading

E-mail threading software groups together an entire chain of an e-mail, identifies the e-mails whose content is wholly contained in later e-mails, and thus allows reviewers to review only (a) the last-best e-mail in a chain and (b) any other e-mails that add something new that is not found in any other e-mail. This technology saves time, increases the consistency of coding, permits better identification of privileged information and speeds up the pace of the review, allowing reviewers to "bulk code" groups of records where appropriate.

Comment 7.c.iii. Keyword Searching

Keyword searching involves searching the documents for words or phrases that are common and distinct to a claim or defence, such as product names and components in a product liability case. Note that, due to the casual nature of many e-mails, potentially relevant e-mails may not contain the words or

phrases selected, as the correspondents are familiar with the context and the exchange is part of a larger conversation. Care should be taken when selecting keywords, and the results of keyword searches should always be validated through sampling both the responsive and nonresponsive populations.

Comment 7.c.iv. Predictive Coding/Machine Learning Systems/Technology Assisted Review

Predictive coding, machine learning or technology assisted review is a combination of technology and workflow that assists in prioritizing records in a data set for review. The basic premise is that a person (ideally, a senior lawyer) familiar with the key issues in a case will "train" the computer to identify relevant records through a basic relevant/not relevant triage phase. Workflows and technology may vary in that the initial records may be a random sample, or the computer may be fed relevant records in a "seed set."

Once the computer confirms it has sufficient information to code the records the same way that the trainer would code the records, it ranks the remaining un-coded records by likelihood of being relevant. This permits the lawyers to prioritize the balance of the records for review, concentrating on the records most likely to be relevant first. In some cases, it may be reasonable and defensible to not review some of the remaining data set, given the low probability that it contains any relevant records.

While this is still an evolving field, with significant efforts being made to assess the capabilities of these still-evolving analytics technologies (including predictive coding and other forms of auto-classification), it is fair to say that these tools, when used by skilled practitioners as part of a process managed by experts, have repeatedly yielded more accurate results than

traditional eyes-on linear review by humans and have done so more quickly and at lower overall cost.

It must be emphasized that the workflow and validation processes are critical when utilizing predictive coding to ensure defensibility, since the algorithms are based on probability and statistical analysis. Predictive coding technology on its own is not a substitute for the legal judgment of review lawyers. It is merely a tool that may be effectively applied in large-volume cases where keywords and other technologies are not as effective.

All of the above tools can significantly increase, not just the efficiency of a document review project, but also its accuracy, and at the same time reduce the overall cost. It can also assist in preventing inadvertent production of privileged or confidential information. As valuable as these tools are, ultimately counsel must ensure that legal judgment and a carefully documented methodology are adopted and that the results of using any tools are validated.[151]

Comment 7.d. Sampling and Validating Results

All discovery processes should be subject to accepted methods of validation as appropriate for the particular circumstances.

One approach used to validate results is sampling. Sampling is the process of examining a subset of a document population and making a determination about the entire population based on that examination. Sampling can be carried out on a tar-

151. *Air Canada v. West Jet*, [2006] 81 OR (3d) 48, 2006 CanLII 14966 (ONSC) [*West Jet*].

geted basis ("purposive" sampling) or systematically ("statistical" sampling). The most appropriate method will depend on the circumstances of each case.

Under Principle 7, sampling—whether purposive or statistical—is an appropriate tool both to limit the initial scope and cost of a discovery project, and to validate the results of a technology assisted review.

For example:

- Where a party possesses a series of backup tapes, it may be appropriate to inspect the contents of a few of the tapes, as a sample, to determine whether the inspection of the remaining tapes is required. In this case, determining what tapes to sample could be a matter of common sense, informed by the client's special understanding of where relevant ESI would be most likely to reside. This situation might therefore call for purposive sampling.[152]
- The above example could also apply to a room full of boxes. Inspecting or sampling a set number of documents from each box may help in determining which boxes may require further review.
- Running search terms on files within a network group share and then sampling the results may help determine that a very low percentage of files within that network group share contain evidence that is relevant. This high cost/low return ratio (or low marginal utility ratio) may

152. See e.g. *McPeek v. Ashcroft*, 212 F.R.D. 33, 37 (D.D.C. 2003).

weigh against the need to search that source further or it may be a factor in a cost-shifting analysis if one party insists that very expensive and time consuming searches be employed. See *Consorcio Minero Horizonte S.A. et al. v. Klohn-Crippen Consultants Limited et al*[153] for an application for the concept of cost shifting in an analogous situation.

- During a review, the legal team identifies a pattern of records that are consistently irrelevant. Using keyword searching, a large subset of the records is identified as being potentially irrelevant. A statistically valid sample of this subset is reviewed, and no relevant records are identified. Based on this process, it is decided that the subset can be considered irrelevant with no further manual review.

There are two statistical measurements that are typically used to measure the results of a sample analysis: recall and precision.

i. **Recall.** The percentage of relevant records that are identified out of all relevant records in the population.

- If a collection has 100 relevant records and the analysis found 50 of them, the recall would be 0.5 or 50%.
- Recall measures how completely a process has captured the target set. High recall means that there were very few relevant documents that

153. 2005 BCSC 500 (CanLII).

were not found (false negatives); low recall indicates a higher proportion of false negatives.

- Higher recall supports the position that a party has met its production obligations.

ii. **Precision.** The percentage of documents retrieved that are in fact relevant.

- If 50 records are identified as relevant, but 5 of them turn out to be non-relevant, the precision is 0.9 or 90%.
- Precision measures how well a process has avoided including irrelevant records. High precision means there are very few documents in the result set that are not relevant (false positives); low precision indicates a higher proportion of false positives.
- A higher precision rate helps avoid reviewing too many irrelevant records.

The goal is to achieve both high recall and high precision.

Regardless of the technology used, or whether the documents are in paper or electronic format, a consistent method for selecting a sample and analyzing the results must be developed. This "consistent" method need only be consistent within a given set of records—each matter will have a set of documents with its own characteristics. As such, a method suitable for one matter may not be applicable to a different, albeit similar matter.

Principle 8. The parties should agree as early as possible in the litigation process on the format, content and organization of information to be exchanged.

Comment 8.a. Electronically Stored Information Should Be Produced in Electronic Format (Not Paper)

When at all possible, the production of ESI should be made in searchable electronic format,[154] unless the recipient is somehow disadvantaged and cannot effectively make use of a computer.[155] Examples of searchable electronic formats include native files (such as Microsoft Word, Microsoft Excel and Microsoft Outlook files) and imaged representations of the native files converted to a format (such as TIFF[156] or PDF[157]) in a searchable format.

---

154. *Discovery Task Force Guidelines*, *supra* note 92: "Production of voluminous documentation in a form that does not provide meaningful access should be avoided." See also *Cholakis, supra* note 36 at para 30, 44 CPC (4th) 162 (MBQB): "The interests of broad disclosure in a modern context require, in my view, the production of the information in the electronic format when it is available."

155. In a criminal case, in circumstances where the accused was in prison and had insufficient access to computers, the Crown was ordered to disclose in paper form. See *R v. Cheung*, 2000 ABPC 86 (CanLII) at para 99, 267 AR I79: "[W]hile electronic or soft copy disclosure may now in the 21st Century be considered a usual form also, in the circumstances of this case, it is not accessible to the accused."

156. TIFF stands for "Tagged Image File Format." It is a computer file format for exchanging raster graphic (bitmap) images between application programs. A TIFF file can be identified as a file with a ".tiff" or ".tif" file name suffix.

157. PDF stands for "Portable Document Format." It is a file format used to present documents in a manner independent of application software, hardware and operating systems. A PDF file can be identified with a ".pdf" file name suffix.

The practice of producing ESI in static format such as paper should be discouraged in most circumstances for several reasons:

- Depending on the nature of the electronic record, paper may not be an authentic substitute for the contents and properties of the original record.
- Paper cannot retain potentially critical metadata (such as who the author was, the date the document was created, the date the document was last modified), which, if relevant, is producible.
- Paper records are harder to search and are harder to logically organize using litigation support software tools. This means that a paper production set is usually less meaningful than a set of documents produced in a searchable electronic format.[158]
- Reviewing a large collection of paper records is more time-consuming and expensive than re-

158. See *Servier, supra* note 111 at para 10: "Following this contrary approach, the defendants took the position in the first instance that the CD-ROMs and electronic database (used in conjunction with the *Summation* legal data processing system) defendants' counsel had prepared at significant expense for themselves in respect of their own documents (so as to organize meaningfully the documents they disclosed in their affidavits) were not to be shared with the plaintiff. Later, in the course of a case conference, the defendants provided an index in word format but plaintiff's counsel asserted that the voluminous documents were simply not searchable. The production of voluminous documentation in a form that does not provide meaningful access is not acceptable." *Solid Waste Reclamation Inc. v. Philip Enterprises Inc.* (1991), 2 OR (3d) 481 (CanLII) (Gen Div.).

viewing the same collection of searchable electronic records,[159] since parties will then not be able, in their review, to take advantage of technologies that can greatly enhance review efficiency and search accuracy.

- Each printed set required for hard copy production adds to the cost of reproduction, shipping and storage, whereas multiple electronic copies can be made at a nominal cost. The use of electronic productions creates opportunities for cost sharing, particularly in multi-party actions, where savings can be significant.
- Producing documents in electronic format is better for the environment.

Comment 8.b. Agreeing on a Format for Production

The parties should agree on how they are going to produce documents at the early stages of litigation or during discovery plan conferences. It is preferable if each party designates the form in which it wishes ESI to be produced. Given the fact that there are so many different litigation support programs available today, each party may have different production requirements. While it is acceptable for the parties to produce documents in different formats, it is strongly recommended that

159. See *Sycor, supra* note 111. Where the cost of printing and photocopying e-mail for production was estimated at $50,000, "[a]t the very least there should be consideration given to electronic production of documents that are required and perhaps the use of computer experts to identify what exists and what is truly relevant to the issues that are actually in dispute."

parties develop a framework for resolving disputes over the form of production.[160]

For a number of reasons, ESI should wherever possible be produced in native format. First, the native version is the truest, most accurate version of the document; second, native files are easier, faster and cheaper to transfer, upload and search than are any other format; third, conversion to other formats entails the loss of information; and fourth, native versions contain all of the application-level and user-created metadata for the files, some of which may be crucial to understanding the true meaning of the files. User-generated metadata is information about the document that is entered by a user at the file level—for example, the fields that can be populated in the Properties tab of a Microsoft Office document. In addition, many kinds of electronic files contain information that can be lost if it is simply converted to an image or other non-native format. Examples of such information include that which is: (a) in spreadsheets: macros, formulas, conditional formatting rules and hidden columns/rows/worksheets; (b) in presentations: speaker notes; (c) in word-processing documents: text-editing notations ("track changes"); and (d) in virtually all file types: comments, sticky notes and highlighting. Such information is as much a part of the document as the visible text and, in some investigations or litigation, could be highly relevant. Parties should therefore be prepared to produce files in native format or explain why they prefer not to. Parties should also be aware that most modern native file processing tools can extract metadata that indicates

160. *Kaymar, supra* note 119. The Master observed that a well-crafted discovery plan that contains dispute resolution mechanisms can avoid motions practice, including on issues such as the format of production.

whether an individual file contains this kind of normally-hidden information and that these metadata fields (e.g. "contains hidden text") can be provided as part of the production.

Where parties prefer to receive files converted from native format to an image format—such as PDF or TIFF—they should so specify. The fact that one party prefers to receive documents in PDF/TIFF format, however, does not preclude another party from asking that the production to it be made in native format.[161] It is customary and acceptable practice to convert documents that are to be redacted into image format, but parties producing redacted images should make sure that the rest of the document is searchable, by performing optical character recognition (OCR) on the redacted images and including the resulting text in the production.

Where parties do not specify a form of production, or where a producing party objects to a requested form of production, the producing party should notify the other party of the form in which it intends to produce the information. It is recommended that production occur either (1) in the form in which the information is ordinarily maintained or (2) in a reasonably usable form. It is rarely appropriate to downgrade the usability

161. *Quizno's*, *supra* note 127 at paras 128–131. The Court disagreed with the defendant's refusal to re-produce copies of Excel documents in Excel format. The documents had originally been produced in TIFF format pursuant to the discovery plan. There would be no hardship to the defendant to produce the Excel files. The Court found ". . .generally speaking a court should not allow the significant effort to establish a plan becoming a waste of time and effort by not holding parties to their agreement, discovery plans are just that, they are a plan and there is an old maxim that it is a bad plan that admits of no modification." (para 130) The Court ordered copies of the already produced documents, if readily available, to be produced again in Excel format.

or searchability of produced information without the consent of the receiving party or an order of the Court.

There is also an expectation that trials will increasingly be conducted electronically (which requires that documents be produced in an electronic format). In *Bank of Montreal v. Faibish*,[162] the Court rejected the proposition that the trial be conducted both through paper and digital information. "Paper must vanish from this Court and, frankly, the judiciary cannot let the legal profession or our court service provider hold us back."[163]

Comment 8.c. Affidavits and the Format and Organization of Record Lists

Court rules in most provinces require the preparation of a list that describes all relevant documents, with information to permit individual documents to be separately identified. Depending on the province, this might be called an affidavit of documents, affidavit of records, affidavit disclosing documents or list of documents.[164] The applicable rules of court may also require the parties to provide a list of documents that may be relevant but are not within the care and control of the producing party, and a list of documents that are being withheld on the basis of privilege.

---

162. 2014 ONSC 2178.

163. Although this type of decision was rare at the time of the drafting and publication of this edition of *The Sedona Canada Principles Addressing Electronic Discovery*, it is anticipated that this type of decision and order will be made more common in the future.

164. Such lists are called an affidavit of records in Alberta, and an affidavit disclosing documents (individual/corporation) in Nova Scotia. In all other provinces that have this requirement it is known as ether an affidavit of documents or list of documents.

The requirement for the above dates back to an era when parties produced only paper documents. The document list was the only method of providing organization to a paper collection. This practice remains today, although as noted further below, it is evolving.

Where parties exchange paper productions or electronic productions of paper records which have been digitized, the document lists are usually manually coded using information obtained from the (face) content of the record. The standard fields exchanged typically include: Production Number; Record Type; Author; Recipient(s); Date; Document Title; or Subject; and, sometimes, Page Count.

When creating such lists (either for paper or native productions), parties should consider using the metadata associated with electronic records to populate the above standard fields instead of manually coding information from the content of the record, even if the original native files are converted to an image format prior to production. This practice is particularly applicable to the production of e-mails, where the metadata clearly indicates the Record Type, Author, Recipient(s), Record Date and Record Title (subject). For non-e-mail records, the metadata, file type or file-extension value can be used to denote the Record Type, the filename or pathname could represent the Record Title and last modified timestamp could represent the Record Date. The suitability of using metadata instead of manually coded information should be based on whether using the metadata will result in the production of information sufficient to uniquely identify each record being produced.

As noted above, the need to provide these "Lists of Documents" is evolving, given the nature of electronic documents and the ways they can be searched and sorted. In *Cameco Corp.*

v. Canada,[165] the respondent had argued that the use of metadata to describe all documents was unsatisfactory and had resulted in a "maldescription" of the documents. In some cases, the Author and Date information obtained from the metadata differed from the Author and Date information on the face of the document. The respondent noted that it would be more helpful to have only the document identifier in the list of documents with no author and no date, with which the Court agreed. "So long as the appellant has provided sufficient description of the documents using a numerical identifier for each document, its identification of the document is satisfactory."

Document lists often are part of an Affidavit of Documents that must be sworn by clients verifying that all relevant documents have been produced. In light of the volume of ESI available for discovery in modern litigation, and the fact that it is impossible to verify that all relevant documents have been produced, courts and rules committees may have to reassess the utility of affidavits verifying full disclosure of records. In all cases, the affidavits should be carefully reviewed in order to ensure that the content of the affidavit can be sworn or affirmed by the client, particularly in circumstances where the affiant may not have personal knowledge of the efforts involved in the collection, processing and review of the documents exchanged in production.

165. 2014 TCC 45 (CanLII).

Principle 9. During the discovery process, the parties should agree to or seek judicial direction as necessary on measures to protect privileges, privacy, trade secrets and other confidential information relating to the production of electronically stored information.

Comment 9.a. Privilege

Solicitor-client privilege is intended to facilitate and encourage full and frank communication between a lawyer and client in the seeking and giving of legal advice. Litigation privilege is intended to secure for the litigant a zone of privacy within which to prepare its case against opposing parties. A party potentially waives the solicitor-client privilege, litigation privilege or both if that party, or even a third party, voluntarily discloses or consents to the disclosure of any significant part of the matter or communication, or fails to take reasonable precautions against inadvertent disclosure. Due to the ever-increasing volume of ESI that is potentially relevant, there is an increased risk of the inadvertent disclosure of privileged information. Notably, the privilege review phase can be the most expensive phase of discovery.

Comment 9.a.i. Inadvertent Disclosure

Canadian courts have generally accepted that inadvertent disclosure does not waive solicitor-client privilege.[166] Nev-

166. See *Elliot v. Toronto (City)* (2001), 54 OR (3d) 472 (SC) at para 10 (CanLII); John Sopinka, Sidney N. Lederman & Alan W. Bryant, THE LAW OF EVIDENCE IN CANADA, 2d ed. (Toronto: Butterworths, 1999) at 766–67; *Dublin v. Montessori Jewish Day School of Toronto*, 2007 CarswellOnt 1663 (SCJ); *Sommerville Belkin Industries Ltd. v. Brocklesh Transport and Others* (1985), 65 BCLR 260 (SC) (CanLII); *National Bank Financial Ltd. v. Daniel Potter et al.*, 2005 NSSC

ertheless, one Court held that the privilege was lost after inadvertent disclosure of a privileged communication, deciding that it was possible to introduce the information into evidence if it was important to the outcome of the case and there was no reasonable alternative form of evidence that could serve that purpose.[167] In contrast, see *L'Abbé v. Allen-Vanguard Corp.*,[168] in which the Ontario Superior Court of Justice held that truly inadvertent disclosure should not be treated as waiver of privilege unless the party making the disclosure is truly reckless or delays in reasserting the privilege or certain other conditions are met. Privilege may be lost through inadvertent disclosure based on considerations including: the manner of disclosure, the timing of disclosure, the timing of reassertion of privilege, who has seen the documents, prejudice to either party or the requirements of fairness, justice and search for truth.[169]

The issue of volume was also addressed in *L'Abbé v. Allen-Vanguard Corp.* where the Master held that court inspection

---

113, 233 NSR (2d) 123 (CanLII) [*Daniel Potter*]; *National Bank Financial Ltd. v. Daniel Potter*, 2004 NSSC 100, 224 NSR (2d) 231 (CanLII); *Autosurvey Inc. v. Prevost*, [2005] OJ No 4291 (CanLII) (ONSC).

167. See *Metcalfe v. Metcalfe*, 2001 MBCA 35 at para 28, 198 DLR (4th) 318 (CanLII).

168. See *L'Abbé, supra* note 51. See also *Minister of National Revenue v. Thornton*, 2012 FC 1313 (CanLII) and *McDermott v. McDermott*, 2013 BCSC 534 (CanLII).

169. The Federation of Law Societies Model Code of Professional Conduct, October 2014, Rule 7.2-10, provides: A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent must promptly notify the sender. http://flsc.ca/wp-content/uploads/2014/10/ModelCodeENG2014.pdf. This principle has been adopted by Law Societies in Canadian jurisdictions. See e.g. *Aviaco International Leasing Inc. v. Boeing Canada Inc.*, 2000 CanLII 22777 (ON SC), at para 10–13.

of 6,000 inadvertently produced documents over which privilege was claimed was not a viable option. Instead, the Master placed the obligation of narrowing the dispute in relation to those documents on the parties. In so doing, he directed the parties to first try to reach a meeting of the minds with respect to probative value and relevance of the documents and then to attempt to come to agreement on categories of the documents that should be available at trial. Finally, once the number of documents was reduced, the parties were to consider what process could be used to filter the documents for relevance and privilege, including considering technological solutions. The Master held that "cost effectiveness, practicality and privilege should be the touchstones. The exercise should be governed by the '3Cs' of cooperation, communication and common sense."[170]

Comment 9.a.ii. Protective Measures

With the extremely large numbers of electronic documents involved in litigation matters, conducting a review of relevant electronic documents for privilege and confidentiality can be very costly and time consuming. Parties must employ reasonable, good-faith efforts[171] to detect and prevent the production of privileged materials. Good-faith efforts will vary from case to case, ranging from a manual page-by-page review for a small data set, to an electronic search for words or phrases likely to locate privileged materials where the data set is larger. In many cases, a combination of the two is appropriate. Other technological tools such as predictive coding and concept clustering

170. *L'Abbé, supra* note 51 at para 98.

171. See *West Jet, supra* note 151 at para 20, where the Court rejected the request for an order protecting against the waiver of privilege where a "quick peek" type of production was being proposed. But see also *L'Abbé, supra* note 51.

may also assist with the identification and segregation of potentially privileged records.

Comment 9.a.iii. Sanctions

Courts have imposed a spectrum of sanctions when counsel has obtained and reviewed privileged communications from an opposing party without that party's consent. These sanctions can include striking pleadings, the removal of counsel from the file and costs. The removal of counsel has been ordered where the evidence demonstrated that, despite the fact counsel or the party knew or should have known that it had acquired an opposing party's solicitor-client communications, counsel took no steps to seek directions from the Court or to stop the review and notify the privilege holders.[172]

Comment 9.a.iv. Use of Court-Appointed Experts

In certain circumstances, a court may appoint a neutral third party (i.e. a special master, judge or court-appointed expert, monitor or inspector) to help mediate or manage electronic discovery issues.[173] A benefit of using a court-appointed neutral expert is the probable elimination of privilege waiver concerns with respect to the review of information by that neutral expert. In addition, a neutral expert may speed the resolution of disputes by fashioning fair and reasonable discovery plans based upon specialized knowledge of electronic discovery or other technical expertise along with the pertinent facts in the case.

172. See *Daniel Potter, supra* note 166; *Auto Survey Inc. v. Prevost*, 2005 CanLII 36255 (ONSC); and *Celanese, supra* note 95.

173. *Catalyst Fund General Partner 1 Inc. v. Hollinger Inc.*, 2005 CanLII 30317 (ONSC).

Where necessary and practical in the circumstances of a particular matter, parties should cooperate and agree upon the appointment of a neutral expert.

The Supreme Court of Canada has endorsed the practice that review of documents seized under an Anton Piller order be undertaken by a lawyer who then prepares a report detailing conclusions reached.[174]

Comment 9.a.v. Protection of Privileged Information

Given the expense and time required for pre-production reviews for privilege and confidentiality, parties should consider entering into an agreement to protect against inadvertent disclosure, while recognizing the limitations in the applicable jurisdiction of such an agreement vis-à-vis courts and third parties. These agreements are often called "clawback" agreements.[175] Court approval of the agreement should be considered. The agreement or order would typically provide that the inadvertent disclosure of a privileged document does not constitute a waiver of privilege. The privileged communication or document should be returned, or an affidavit sworn that the document has been deleted or otherwise destroyed. The agreement should provide that any notes or copies will be destroyed or deleted and any dispute will be submitted to the Court. It is preferable that any such agreement or order be obtained before any production of documents take place. The agreement should clearly specify the process and steps to be taken in the event a party or its counsel determine that a privileged communication has been inadvertently disclosed.

---

174. *Celanese, supra* note 95.

175. See *West Jet*, *supra* note 151; see also *Zubulake v. UBS Warburg* LLC, 216 FRD 280, 290 (SDNY 2003) (WL).

Parties should exercise caution when relying on clawback agreements as such agreements may not eliminate counsel's obligation to use reasonable good-faith efforts to exclude privileged documents prior to initial disclosure. In *Nova Chemicals (Canada) Ltd. v. Ceda-Reactor Ltd.*, a party invoked a clawback agreement concerning inadvertently produced documents, but the Court rejected its argument and set out principles to be considered in such determinations.[176] Also, a clawback agreement may not be enforceable against a party who is not a signatory to the agreement.[177]

In the case of very large data sets, parties to litigation could consider a more aggressive type of clawback agreement, perhaps even agreeing to a reduced pre-production search methodology requirement. Such clawback agreements, however, should be approved by the Court to ensure enforceability.

There is a growing body of evidence from the information-science field that the use of technologically-based search tools may be more efficient and more accurate than manual searches.[178] The Working Group recommends that Courts consider this body of evidence in assessing whether reasonable steps were taken in a privilege review.

---

176. *Nova Chemicals (Canada) Ltd. v. Ceda-Reactor Ltd.*, 2014 ONSC 3995 (CanLII).

177. *Hopson v. Mayor of Baltimore*, 232 FRD 228 (D Md 2005) (WL Can).

178. Feng C. Zhao, Douglas W. Oard & Jason Baron, *Improving Search Effectiveness in the Legal E-Discovery Process Using Relevance Feedback* (paper delivered at the 12th International Conference on Artificial Intelligence and the Law (ICAIL09 DESI Workshop) (2009)); Maura R. Grossman & Gordon V. Cormack, *Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review* (2011), 17:3 Rich JL & Tech 11.

Comment 9.b. Protection of Confidential Information

Confidentiality concerns can arise when there is sensitive or proprietary business information that may be disclosed in discovery. Protective orders can be sought to protect confidential information produced over the course of discovery. The availability of protective orders is the product of an attempt to balance the competing values of an open and accessible court proceeding and the public interest in a fair judicial process against serious risks of harm to commercial interests of one or more litigants.

The seminal decision on this topic is *Sierra Club of Canada v. Canada (Minister of Finance)*,[179] a case involving the judicial review of proceedings initiated by an environmental organization, the Sierra Club, against a Crown Corporation, Atomic Energy of Canada Ltd. ("Atomic Energy"), which concerned the construction and sale to China of nuclear reactors. The Sierra Club sought to overturn the federal government's decision to provide financial assistance to Atomic Energy. At the heart of this decision were confidential environmental assessment reports originating in China, which Atomic Energy sought to protect by way of a confidentiality order. Atomic Energy's application before the Federal Court, Trial Division[180] was rejected, and the appeal from this decision was dismissed by all but one judge of the Federal Court of Appeal.[181] On further appeal to the Su-

179. *Sierra Club of Canada v. Canada (Minister of Finance)* (2002), 211 DLR (4th) 193 (CanLII) (SCC), 2002 SCC 41 (CanLII).

180. *Sierra Club of Canada v. Canada (Minister of Finance)* (1999), 1999 CarswellNat 2187 (FCTD).

181. *Sierra Club of Canada v. Canada (Minister of Finance)* (2000), 2000 CarswellNat 3271 (FCA).

preme Court of Canada, Atomic Energy was ultimately successful in obtaining relief. In arriving at its conclusion, a unanimous Supreme Court reasoned:

> A confidentiality order should only be granted when (1) such an order is necessary to prevent a serious risk to an important interest, including a commercial interest, in the context of litigation because reasonably alternative measures will not prevent the risk; and (2) the salutary effects of the confidentiality order, including the effects on the right of civil litigants to a fair trial, outweigh its deleterious effects, including the effects on the right to free expression, which in this context includes the public interest in open and accessible court proceedings. Three important elements are subsumed under the first branch of the test. First, the risk must be real and substantial, well grounded in evidence, posing a serious threat to the commercial interest in question. Second, the important commercial interest must be one which can be expressed in terms of a public interest in confidentiality, where there is a general principle at stake. Finally, the judge is required to consider not only whether reasonable alternatives are available to such an order but also to restrict the order as much as is reasonably possible while preserving the commercial interest in question.[182]

Also, the long-standing practice of redacting documents to prevent the disclosure of irrelevant, confidential or privileged

182. See head note of *Sierra Club*, *supra* note 179.

communications remains in effect with respect to the production of ESI. The use of redactions to protect confidential or privileged information from disclosure is a tool that should be used, provided that the reason for the redaction is clearly and properly identified. If necessary, parties can obtain an appropriate court order, or incorporate terms into a Discovery Plan, for the redaction of confidential or personal information. The use of electronic tools for redactions should also be considered as such tools can greatly reduce the time and expense associated with manual redaction.

Comment 9.c. Privacy Issues

Confidentiality orders, the common law and civil procedure rules may limit the extent to which commercially sensitive or personal information may be disclosed. Canada and its provinces, to varying extents, have comprehensive privacy legislation[183] governing the collection, use and disclosure of personal

183. Legislation regulating the public sector includes: the *Privacy Act*, RSC 1985, c P-21; *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165; *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25; *Freedom of Information and Protection of Privacy Act*, SS 1990-91, c F-22.0I; *Freedom of Information and Protection of Privacy Act*, CCSM c F-175; *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F-31; *An Act respecting access to documents held by public bodies and the protection of personal information*, LRQ c A-2.1; *Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5; *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05; *Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c F-15.01; *Access to Information and Protection of Privacy Act*, SNL 2002, c A-1.1. Legislation governing the private sector includes the *PIPEDA, supra* note 33; *Personal Information Protection Act*, SBC 2003, c 63; *Personal Information Protection Act*, SA 2003, c P-6.5; *An Act respecting the protection of personal information in the private sector*, LRQ c P-39.1.

information,[184] in both the public and private sectors, that may affect the discovery process. Privacy issues can arise in a wide variety of contexts and can include the privacy rights of non-parties.

The courts have not been sympathetic to objections to producing relevant information based on privacy legislation. Courts do, however, consider privacy issues in assessing whether discovery requests are too broad or whether non-relevant private information can be protected.[185]

It is important to note that the deemed undertaking rule,[186] i.e. the implied undertaking rule, is a rule in the discovery process only; it does not provide privacy protection per se. For example, in Ontario, the deemed undertaking rule only applies to evidence obtained in the actual discovery process, and it specifically does not apply to evidence filed with the court or referred to during a hearing. A court order can also be obtained to relieve compliance with the deemed undertaking rule.[187]

Comment 9.c.i. Social Media

A party should consider whether social media content and documents are relevant and should be preserved and listed in an affidavit or list of documents or records. A court may order private portions of a party's social media profiles and pages to be disclosed where the information is relevant and the probative value of the information justifies the invasion of privacy

184. Generally defined as information about an identified or identifiable individual.

185. See *Dosanjh v. Leblanc*, 2011 BCSC 1660 (CanLII).

186. Generally, the deemed undertaking rule prohibits parties from disclosing evidence and information obtained during the discovery process outside the confines of the litigation.

187. *Ontario Rules*, *supra* note 10, 30.1.01.

and the burden of production.[188] The mere fact however that a party has a social media presence does not presumptively mean that the private aspects of an account are relevant.[189] For example, in *Bishop v. Minichiello*, the defendants sought production of the plaintiff's hard drive to determine the time the plaintiff spent on Facebook.[190] The plaintiff's computer was used by all members of his family. To protect the privacy rights of the non-party family members, the Ontario Court ordered the parties to agree on the use of an independent expert to review the hard drive. In *Fric v. Gershman*,[191] the Supreme Court of British Columbia similarly sought to protect the privacy of third parties when it ordered production of certain photographs posted on the plaintiff's Facebook page. The plaintiff was permitted to edit the photographs prior to disclosure to protect the privacy of other individuals who appeared in them. The Court in *Fric* refused to order production of commentary from the Facebook site, however, holding that if such commentary existed, the probative value of the information was outweighed by the competing interest of protecting the private thoughts of the plaintiff and third parties.[192]

---

188. See *Leduc v. Roman*, 2009 CanLII 6838 (ON SC); *Frangione v. Vandongen*, 2010 ONSC 2823 (CanLII); *Murphy v. Perger*, [2007] OJ No 5511 (WL Can); *McDonnell v. Levie*, 2011 ONSC 7151 (CanLII); and *Casco v. Greenhalgh*, 2014 CarswellOnt 2543 (Master).

189. *Schuster v Royal & Sun Alliance Insurance Company of Canada*, [2009] OJ No 4518 (WL) (ON SC); and see *Stewart v. Kemptster*, 2012 ONSC 7236 (CanLII); *Garacci v. Ross*, 2013 ONSC 5627 (CanLII); and *Conrod v. Caverley*, 2014 NSSC 35 (CanLII).

190. 2009 BCSC 358 (CanLII), leave to appeal for further production dismissed, 2009 BCCA 555 (CanLII).

191. *Fric v. Gershman*, 2012 BCSC 614 (CanLII).

192. *Fric v. Gershman*, 2012 BCSC 614 (CanLII) at para 75, citing *Dosanjh v. Leblanc and St. Paul's Hospital*, 2011 BCSC 1660.

If necessary in the circumstances, social media content and documents should be collected and produced in a forensically sound manner. As an example, screen captures and printed paper versions may be unreliable.[193]

Generally, a lawyer is not permitted to have contact with a represented opposing party without the party's counsel present. The lawyer needs to keep that rule in mind if reviewing social media of an opposing party. The social media site may advise the opposing party that the lawyer has viewed the site, and, if counsel has gone beyond merely viewing publicly available pages and has actually engaged with the opposing party in some fashion, such as e-mailing or "friending" that party, this may violate the no-contact rule.

Comment 9.c.ii. Employee Privacy on Employer-Issued Devices

An employee's right to privacy on an employer owned device (e.g. desktop computer, laptop, tablet, or phone) will continue to be a fact-specific determination. In *R. v. Cole*, the Supreme Court of Canada confirmed that employees do have limited privacy rights on employer-issued computer devices.[194] The Court held that employees may have a reasonable expectation of privacy where personal use is permitted or reasonably expected. Ownership and workplace policies were held to be relevant for consideration but not determinative of whether privacy was protected in a particular situation. In *International Union of Elevator Constructors, Local 50 v. Otis Canada Inc.*,[195] the

193. 2013 CanLII 3574 (ON LRB).

194. 2012 SCC 53.

195. *International Union of Elevator Constructors, Local 50 v. Otis Canada Inc*, 2013 CanLII 3574 (ON LRB).

Labour Relations Board held, however, that if an employee chooses to use a company vehicle to and from home, the company is not restricted from using technological devices to monitor the vehicle at all times.

In juxtaposition to the above are the rights of the employer with respect to its proprietary and confidential information when an employee uses his or her own device for work (commonly referred to as a "bring your own device" or BYOD). Many businesses acknowledge and accept the use by employees of employee-owned digital devices on corporate networks. BYOD policies are essential if employees are using their own devices. These policies need to set out who owns the data, and provide a means to allow the organization to gain access to that data if necessary.

Comment 9.c.iii. Criminal Records and Investigations

In cases that involve criminal or regulatory investigations or proceedings, a number of privacy rights arise. The seizure of electronic evidence during a regulatory or criminal investigation or process brings into play the right to be free against unreasonable search or seizure under section 8 of the *Canadian Charter of Rights and Freedoms* ("the *Charter*").[196]

Where the electronic evidence required for a proceeding forms part of a parallel criminal investigation, the principles and screening process identified in *D.P. v. Wagg*[197] should be applied to obtain the appropriate court orders and protections if required. Prior to the release of criminal investigation materials,

196. Everyone has the right to be secure against unreasonable search or seizure. Section 8, *Canadian Charter of Rights and Freedoms*. See e.g. *R v. Cole*, 2012 SCC 53 (CanLII).

197. 2004 CanLII 39048 (ON CA) [*Wagg*].

including the contents of computer hard drives seized by authorities, the Crown must be notified and provided the opportunity to review the materials for third-party privacy and public interest concerns.

Comment 9.d. Data Security

Corporations, public organizations, law firms and individuals are all potential targets for data breaches and the theft or loss of valuable information. To secure the protection of privilege, privacy, trade secrets and other confidential information, parties, counsel and service providers should take reasonable steps to safeguard their own documents and data, and those produced to them by opposite parties.

These steps may include appropriate chain-of-custody processes, secure and limited access to the data, encryption and password protection. Parties must also have appropriate procedures in place to secure the data during production and receipt at the completion of a project.

Appropriate chain-of-custody logs and procedures should be used to maintain the integrity of the data from collection to production in court. The chain of custody should document that: the data has been properly copied, transported and stored; the information has not been altered in any way; and all media have been secured throughout the process. The custody log should also include provision for the return of the data to the client or opposing counsel at the conclusion of the project.

At a minimum, data should be password protected, and preferably two-factor authentication[198] should be required.

198. Two factor identification requires a user to provide two different security components to access information, such as a password and USB stick with a secret token, or a card and a PIN.

Hackers have frequently targeted law firms and may view them as soft targets. In addition to technological security, access should be restricted to those with a "need to know," and both physical storage facilities and computer servers should be secured from unauthorized access.

Comment 9.e. Document Lists—Producing Coded Information

In some cases, courts have required the producing party to produce not only electronic records but also the objective coding created by the producing party when processing its records.[199] Producing selected contents of a litigation database, however, should not be confused with producing the software used to create and manage the database, which courts generally have not required.

The following decisions may assist counsel in understanding the Canadian approach to these issues.

- In *Wilson v. Servier Canada*,[200] the Court granted the plaintiff's motion for an order directing the defendant to release the objective coding of the documents in their litigation support database in order to meaningfully satisfy its disclosure requirements, given the volume of documents.
- In *Logan v. Harper*,[201] the defendants had produced the documents along with a searchable

199. For a discussion of coding, including a definition of objective coding, see *supra*, Introduction, section F.8 ("Advanced Technology Can Help to Organize, Search and Make Sense of ESI") and note 27.

200. *Servier, supra* note 111.

201. *Logan, supra* note 125.

index in electronic form. The index did not permit full-text searching of the documents, although the version of the application used by counsel for the defendants did offer that feature. The Master considered litigation support and document management software not normally subject to disclosure, and accepted as reasonable that the plaintiff's counsel purchase a licence for the software for access to the full-text search feature.

- In *Jorgensen v. San Jose Mines et al.*,[202] the defendants sought delivery of the electronic database used by the plaintiff to compile the list of documents. In this case, the Court ordered the plaintiff to provide a copy of the database to the defendants in electronic format and ordered the defendants to pay $4,000 to the plaintiff's firm as a reasonable proportion of the costs of preparing the database.
- More recently, however, in *Gamble v. MGI Securities Inc.*,[203] the Ontario Superior Court ordered all relevant Summation load files be delivered to the plaintiff in a DVD format, as requested by the plaintiff, at no cost above that of a blank DVD, rejecting the defendant's argument that the plaintiff should share in some of the costs resulting from preparing, coding and scanning the documents into the litigation support database. The Court noted that cost sharing may be

202. 2004 BCSC 1653 (CanLII).

203. 2011 ONSC 2705.

> warranted in some circumstances, but that various circumstances militated against it in this case, including the fact that the defendant had scanned many more documents than what were ultimately deemed relevant and the wide discrepancy between the financial abilities of the two parties—the plaintiff being a former employee of the corporate employer. It is noteworthy too that the Court accepted the plaintiff's argument that cost sharing in this case would be contrary to Sedona Canada Principle 12 which states that the reasonable costs of producing, collecting and viewing of documents to be produced will normally be borne by the producing party.[204]

Principle 10. During the discovery process, the parties should anticipate and respect the rules of the forum or jurisdiction in which the litigation takes place, while appreciating the impact any decisions may have in related proceedings in other forums or jurisdictions.

A single subject matter may give rise to proceedings in different forums (e.g. civil court, criminal court, arbitration, administrative or regulatory hearing) or jurisdictions (e.g. local, provincial, federal and other nations such as the U.S., Europe and elsewhere). Even within a single jurisdiction, there may be several related proceedings in different forums to which distinct discovery rules apply. These proceedings may take place concurrently or at different times.

---

204. *Ibid*.

In any proceeding, counsel must comply with specific discovery rules applicable to the particular forum or jurisdiction. Counsel need to appreciate that the rules of discovery across the applicable forums or jurisdictions may be in conflict with each other. In Canada alone, the rules of discovery vary among the common law provinces, and the discovery process in Quebec differs from discovery processes in the common law provinces. For example, in Ontario, "relevant" documents must be produced, whereas, in Alberta, "relevant and material" documents must be produced. In addition, there are some significant procedural and substantive differences in the discovery process, and in the privilege, privacy and evidence rules, between Canada and the United States.

Accordingly, when there are related proceedings, counsel must make good-faith efforts to ensure that there are no breaches of the rules of any applicable forum or jurisdiction. Counsel should take care to fully explain to clients the governing discovery process in the forum or jurisdiction so that the clients can make informed decisions on how to proceed. This requires counsel to take a proactive approach at the earliest possible stage in a proceeding to ensure that clients are not compromised in one forum or jurisdiction by actions taken in another.

The recommended cooperative process offers an ideal opportunity to identify and resolve any possible forum related rules conflicts at the earliest stage of a matter when possible. While negotiating a discovery plan, counsel should also consider how efforts can be coordinated to reduce the duplication of work so that the preservation, collection, review and production of ESI and other documents for all related matters can occur in the most cost-effective manner.

Comment 10.a. Geographic Jurisdictions and Cross-Border Litigation

When there is related litigation in other geographic jurisdictions, counsel should identify and consider the implications of the differences in procedural and related substantive law. While not intended to provide a comprehensive discussion, the following issues should be considered in any cross-border litigation matters:

i. **Procedure.** The procedures regarding the timing of discoveries, the need for discovery plans and the process for handling undertakings and refusals on discovery can often be very different.

ii. **Scope of Discovery.** The scope of what is discoverable and the obligations to produce can vary greatly between jurisdictions, including whether there is a positive obligation to produce relevant evidence versus producing documents in response to a written request.

iii. **Custody, Possession, Power or Control.** Production obligations can extend to documents not in the custody or possession of a party, but in their power or control, including documents held by a third-party "cloud" service provider, perhaps in a different jurisdiction. For example, if a party located in Canada has relevant documents stored on a server in Europe and can retrieve those at any time by logging in or asking for them, those records will likely be subject to an obligation to produce.

iv. **Affidavit of Documents.** The responsibility for swearing or affirming the completeness of the collection of documents produced in the proceeding can vary by jurisdiction and can affect the decisions regarding a proportionate discovery plan. Counsel and the client may have

different risk analyses regarding the steps to be taken to preserve and produce documents.

v. **Deemed Undertaking and Subsequent Use.** The deemed undertaking rule that exists in many Canadian provinces does not exist in the U.S. Counsel should consider the need for consent, and for protective or sealing orders, regarding subsequent use of information disclosed in the course of the discovery process. Orders in the foreign jurisdiction may be required to protect the deemed undertaking in cross-border litigation.

vi. **Non-Parties.** The process to obtain relevant evidence and documents from non-parties varies greatly among jurisdictions. In the common law provinces, non-parties can only be examined with leave of Court, and while a non-party's documents can be compelled prior to trial, the process to obtain such orders is very different from requesting documents from a party.

vii. **Privacy and Confidentiality.** Privacy laws in foreign jurisdictions can be very different. This includes the expectation of privacy and the privacy afforded to employees on employer-issued devices and computers. The legal test and process for obtaining protective and sealing orders can also vary significantly. Obligations pursuant to privacy legislation also need to be considered for cross-border data transfers and processing.

viii. **Privilege.** While most jurisdictions provide some protection to solicitor/client communications, the availability and scope of other privileges (e.g. "litigation" or "work product" privilege, privilege protection for communications with in-house lawyers, privilege protection for settlement negotiations, and the common-interest privilege) can vary significantly in foreign jurisdictions. Waiver of

privilege and counsel's obligation regarding inadvertently disclosed privileged documents also vary in foreign jurisdictions. Counsel should be aware of the variations in privilege rules so as not to inadvertently waive privilege in another jurisdiction.

ix. **Costs.** Rules regarding costs relating to discovery, disclosure and the proceeding differ in foreign jurisdictions. Further, the availability of "cost shifting" will vary from jurisdiction to jurisdiction.

x. **Specific E-Discovery Provisions.** Foreign jurisdictions have different protocols, preservation standards and expectations for electronic discovery. Proportionality and obligations for discovery plans are not principles shared by all jurisdictions. Sanctions can vary in severity as well as the activities or misconduct that would attract sanctions. Some jurisdictions have specific requirements concerning the format or the electronic searchability of the production of e-documents. It is also important to remember that The Sedona Conference's principles addressing electronic discovery also differ between Canada and the U.S. to reflect the different legal systems and rules.

In addition, in cross-border litigation, it may be necessary to obtain documents or information from outside the jurisdiction. The procedure and legal tests for obtaining that evidence can vary. For further information, counsel should consult *The Sedona Canada Commentary on Enforcing Letters Rogatory*, which contains a succinct summary of the key differences in the

rules governing cross-border evidence in Canada and the United States.[205]

The Sedona Conference® International Overview of Discovery, Data Privacy and Disclosure Requirements also provides an overview of discovery and data privacy laws in a number of countries around the world.[206]

Comment 10.b. Forums

Different procedural and substantive laws can also apply in different forums within the same geographic jurisdiction. One common example is in cases involving allegations of securities fraud, which may involve parallel bankruptcy proceedings, criminal proceedings and regulatory proceedings within the same jurisdiction.

Where there are parallel administrative, regulatory or criminal proceedings in the same jurisdiction, counsel should make good-faith efforts to become informed of any procedural and legal differences in disclosure and protection. As with cross-border disclosure, counsel should ensure appropriate protection orders or consents are in place prior to cross-forum disclosure. A proactive approach to obtain the necessary orders or consents will decrease the time and costs of any coordination required.

---

205. The Sedona Conference, *The Sedona Canada Commentary on Enforcing Letters Rogatory Issued by an American Court in Canada: Best Practices & Key Points to Consider* (June 2011 public comment version), online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/463>.

206. The Sedona Conference, *International Overview of Discovery Data Privacy and Disclosure Requirements* (2009), online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/62>.

Comment 10.b.i. Seized Evidence and Investigation Materials in Criminal or Regulatory Investigations

Criminal investigation materials can include a broad range of compelled evidence, the improper disclosure of which can impact privacy rights, privilege rights, the criminal justice system, Crown immunity and the administration of justice. When electronic evidence is seized in the course of a regulatory or criminal investigation, potential issues arise regarding section 8 of the Canadian Charter of Rights and Freedoms and an accused's right to a fair trial.[207] Where electronic evidence has been seized, warrants and various search and seizure provisions of the *Criminal Code* can be implicated.[208]

Materials seized pursuant to warrant or other regulatory compulsion will often be much broader in scope than what would be disclosed in a civil proceeding. Where the requested electronic evidence forms part of a parallel criminal investigation, prior to use or disclosure in any other proceeding, the principles and screening process identified in *D.P. v. Wagg*[209] should be applied to obtain the appropriate court orders to protect, as necessary, privacy rights and privilege rights.[210] Prior to the dis-

207. See e.g. *Kelly v. Ontario*, [2008] OJ No 1901, 91 OR (3d) 100 (CanLII) (ON SC). At issue in *Kelly* were the seizure of a computer in a child pornography investigation and the claims that the seizure and cross-forum disclosure violated the accused's Charter rights. See also the related decisions *College of Physicians and Surgeons of Ontario v. Peel Regional Police*, 2009 CanLII 55315 (ON SCDC), and *Kelly v. Ontario*, 2014 ONSC 3824 (CanLII) [*College of Physicians*].

208. *Criminal Code* RSC, 1985, c C-46.

209. *Wagg, supra* note 197.

210. The need to obtain consent of the Crown is also required in parallel regulatory proceedings, even where the regulatory body has the statutory

closure of evidence obtained in a criminal investigation, the process identified in *Wagg* requires the Crown to be notified and provided the opportunity to review the materials for third-party privacy and public interest concerns.[211]

Regulatory bodies also have the ability to compel the production of evidence through enforcement provisions in the governing legislation.[212] In addition to the power to compel, the regulatory body may have the power to control subsequent disclosure and use of the compelled evidence.[213] It is important to note, however, that where a regulatory body seeks access to criminal investigation materials, it must also comply with the general principles in *Wagg* and provide the Crown the opportunity to raise public interest concerns that may militate against production.[214]

Matters that involve cross-border criminal or regulatory proceedings require particular consideration of the different

---

ability to compel evidence. See *College of Physician and Surgeons of Ontario v. Peel Regional Police*, [2009] OJ No 4091, 98 OR (3d) 301 (CanLII) (ONSCDC).

211. To obtain and use criminal investigation materials in a civil proceeding in Ontario, a motion pursuant to Rule 30.10 of the *Rules of Civil Procedure* would be brought on notice to the Attorney General.

212. For example, sections 11 through 13 of the Ontario *Securities Act*, RSO 1990, c S.5, and sections 142–144 of the British Columbia *Securities Act*, RSBC, C 418, provide for the issuance of Investigation Orders and the appointment of an investigator, and also outline the power of the authority to compel evidence.

213. For example, Ontario *Securities Act*, *supra* note 212, s 16–18, and *BC Securities Act*, RSBC, 1996 c 418, s 148, gives the respective Commissions the ability to limit and place restrictions on the subsequent disclosure or use of the seized evidence.

214. *College of Physicians and Surgeons of Ontario v. Metcalf*, (2009) 98 O.R. (3d) 301, 2009 CanLII 55315 (ON SCDC), see paras 68–77.

self-incrimination and procedural protections afforded to witnesses. For example, witnesses in Canada are entitled to protection under section 15 of the *Canada Evidence Act* and related provincial legislation,[215] which restricts the use of compelled testimony in other proceedings. In such cross-border situations, the Court may impose terms on any orders compelling the protected evidence.[216]

Comment 10.b.ii. Arbitration

Compared to domestic court litigation, the scope of document production is generally narrower in arbitration proceedings.

Particularly in international arbitration, and subject to the rules specified in the arbitration agreement, a party is typically required to produce only the documents upon which it relies and those responsive to focused requests made by the other party. Some assistance in defining an appropriate standard for document production in arbitration may be derived from the International Bar Association's *Rules on the Taking of Evidence in International Arbitration* (the "*IBA Rules*").[217] Article 3 of the *IBA Rules* provides an "admirably clear" process by which requests for documents are made, the requested documents are either produced or objection is made to the request, and any remaining disputes are resolved by the tribunal—importantly, and

215. *Canada Evidence Act*, RSC 1985, c C-5; see also the *Ontario Evidence Act*, RSO 1990 c E.23.

216. See e.g. the principle in a civil case, *Treat America Limited v. Nestle Canada Inc.*, 2011 ONSC 617 (CanLII); and *Treat America Limited v. Nestlé Canada Inc.*, 2011 ONCA 560 (CanLII).

217. *IBA Rules on the Taking of Evidence in International Arbitration* (29 May 2010), online: International Bar Association <www.ibanet.org> [*IBA Rules*].

consistent with the *Sedona Canada Principles*, against a clear standard of both relevance and materiality to the outcome of the dispute, as well as considerations of proportionality and burden.[218] The *IBA Rules* provide that a party seeking document production in an arbitration should frame the request with some precision, ideally identifying particular documents but at least referring to the desired category of documents. Unless the mere fact of the other party's possession of the documents is relevant, only documents that are not otherwise available to the requesting party from other sources should be sought.[219]

While the scope of production in domestic arbitration proceedings more frequently approaches that of domestic court litigation, the flexibility of the arbitral process provides the opportunity to more readily limit document production in accordance with principles of proportionality. Indeed, although the *IBA Rules* were developed in the international commercial arbitration context, "the rules provide a very helpful framework for the production and exchange of documents in any arbitration, whether international or domestic."[220]

With respect to the production of electronic information, the commercial arbitration field faces much of the same pressures as the litigation field, as commentators have noted.[221] Fortunately, the flexibility that is inherent in the arbitral process, if

---

218. Nigel Blackaby and Constantine Partasides, *Redfern and Hunter on International Arbitration*, 5th ed. (Oxford: Oxford University Press, 2009) at 6.108.

219. *IBA Rules*, *supra* note 217 at art 3.

220. J. Brian Casey, *Arbitration Law of Canada: Practice and Procedure*, 2nd ed. (Huntington, New York: JurisNet LLC, 2011) at 204.

221. See e.g. Richard D. Hill, *The New Reality of Electronic Document Production in International Arbitration: A Catalyst for Convergence?* (2009) 25:1 Arb.

harnessed by counsel and arbitrators, may assist in managing the issue more effectively. The *Sedona Canada Principles* provide a useful framework for addressing these issues in the arbitration context. Indeed, referring to the Sedona Conference's *Sedona Principles*,[222] developed for a United States audience, one commentator has observed that they "reflect the concern of the *IBA Rules* for reasonableness and proportionality, avoiding overly burdensome document production requests, and permitting data sampling, searching and selection criteria to be employed to satisfy a party's good-faith obligation to produce."[223]

Parties engaged in arbitration proceedings should be aware that, while the scope of their production obligation may be more limited, it may be important to account for possible other proceedings in which the scope of that obligation may be broader. Efficiencies of scale and scope can be obtained by integrating those other proceedings with the project plan developed for the arbitration proceedings. Conversely, projects developed to collect and process ESI for litigation proceedings should account for and include both the categories of ESI likely to be relied upon by the party in related arbitration proceedings, and the ESI that can reasonably be anticipated to be requested by other parties in the arbitration proceedings. While the actual

---

Intl at 87; and Robert H. Smit & Tyler B. Robinson, *E-Disclosure in International Arbitration*, (2008) 25:1 Arb Intl at 105.

222. See The Sedona Conference, *The Sedona Principles Addressing Electronic Document Production, Second Edition* (2007), online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/81> [*U.S. Sedona Principles*].

223. Richard D. Hill, *The New Reality of Electronic Document Production in International Arbitration: A Catalyst for Convergence?* (2009) 25:1 Arb Intl at 93. See also Nigel Blackaby and Constantine Partasides, *Redfern and Hunter on International Arbitration*, 5th ed. (Oxford: Oxford University Press, 2009) at 6.117–6.123.

scope of production may be more limited in arbitration proceedings, the initial scope of preservation and collection generally does not differ materially in practice.

Principle 11. Sanctions should be considered by the Court where a party will be materially prejudiced by another party's failure to meet its discovery obligations with respect to electronically stored information.

In certain circumstances, when parties fail to meet their discovery obligations for ESI, the fair administration of justice may be undermined. Absent appropriate sanctions for intentional, bad faith or reckless destruction or non-production of electronic evidence, the advantages that a party may receive from such conduct (e.g. having actions brought against them dismissed for lack of evidence or avoiding potential monetary judgments) may create inappropriate incentives regarding the treatment of ESI.

Not all non-production is intentional or the result of bad faith or recklessness. Given the continuing changes in information technology, the volatility and rapid obsolescence of certain forms of ESI and the burdens and complications that will inevitably arise when dealing with growing volumes of ESI, litigants may inadvertently fail to fully preserve or disclose all relevant material. In considering the impact of non-preservation or non-production, the role of the Court is to weigh the context, scope and impact of nondisclosure and to impose appropriate sanctions proportionate to the culpability of the non-producing party, the prejudice to the requesting party and the impact that the loss of evidence may have on the Court's ability to fairly dispose of the issues in dispute.

In some cases, it will be important to distinguish between penalties imposed for deterrent purposes on a wrongdoer whose conduct has resulted in spoliation or non-production,

and remedies made available to the requesting party who may have been prejudiced, even without any intent or ill will on the part of the responding party. Courts should be flexible in tailoring penalties and remedies to suit the particular case.

Comment 11.a. The Law of Spoliation

In the common law provinces in Canada, the common law that governs the destruction of evidence (i.e. spoliation) continues to develop, particularly as its principles apply to ESI. The law of spoliation originates from the principle of "*omnia praesumuntur contra spoliatorem*," an evidentiary principle that permits a court to draw a negative inference against a party that has been guilty of destroying or suppressing evidence.[224]

In Nova Scotia, the rules of civil procedure have been amended to include provisions that expressly deal with the duties to preserve and disclose electronic information, and the consequences of their breach.[225]

---

224. *Zahab v. The Governing Council of the Salvation Army in Canada et al* (2008) CanLII 41827 at para 20 (ON SC), citing *Prentiss v. Brennan*, [1850] OJ No 283 (Upper Canada Court of Chancery). But see *Gladding Estate v. Cote*, 2009 CarswellOnt8102 at para 36, 55 ETR (3d) 191 (SCJ): The court will only draw a negative inference where there is "real and clear evidence of tampering."

225. Rules 16.13 and 16.15 address destruction of electronic information, providing that deliberate or reckless deletion of relevant electronic information (and related activities) may be dealt with under Rule 88—Abuse of Process. Rule 88 lists various remedies for an abuse of process. Such remedies include an order for dismissal or judgment, an order to indemnify the other party for losses resulting from the abuse and injunctive relief. Nova Scotia *Civil Procedure Rules*, Royal Gazette Nov 19, 2008, online: The Courts of Nova Scotia <http://www.courts.ns.ca?Rules/toc.htm>.

The most comprehensive review of the Canadian jurisprudence on the common law of spoliation is found in *McDougall v. Black and Decker Canada Inc*.[226] In that decision, the Court summarized the Canadian law of spoliation in the following way:

- Spoliation currently refers to the intentional destruction of relevant evidence when litigation is existing or anticipated.[227]
- The principal remedy for spoliation is the imposition of a rebuttable presumption of fact that the lost or destroyed evidence would be detrimental to the spoliator's cause. The presumption can be rebutted by evidence showing the spoliator did not intend, by destroying the evidence, to affect the litigation, or by evidence to prove or defend the case.
- Even where evidence has been unintentionally destroyed, remedies may be available in the Court's rules and its inherent ability to prevent abuse of process. These remedies may include such relief as the exclusion of expert reports and the denial of costs.
- The courts have not yet found that the intentional destruction of evidence gives rise to an intentional tort, nor that there is a duty to preserve evidence for purposes of the law of negligence,

226. 2008 ABCA 353 (CanLII) at para 29.

227. See also *Stilwell v. World Kitchen Inc.,* 2013 ONSC 3354 (CanLII) at para 55 and *Blais v. Toronto Area Transit Operating Authority*, 2011 ONSC 1880 (CanLII) at para 72.

although these issues, in most jurisdictions, remain open.

- Generally, the issues of determining whether spoliation has occurred and what is the appropriate remedy for spoliation are matters best left for trial where the trial judge can consider all of the facts and fashion the most appropriate response.
- Some pretrial relief may be available in the exceptional case where a party is particularly disadvantaged by the destruction of evidence. Generally, this is accomplished through the applicable rules of court, or the Court's general discretion with respect to costs and the control of abuse of process.

As noted, there is an open question as to whether spoliation exists as an independent tort in Canada.[228] The British Columbia Court of Appeal in *Endean v. Canadian Red Cross Society*[229] held that spoliation will not ground an independent tort. The question, however, remains unsettled in other Canadian jurisdictions.

---

228. *See Spasic (Estate) v. Imperial Tobacco Ltd.* [2000] OJ No 2690 (ON CA), 49 OR (3d) 699, 2000 CanLII 17170 (CA) (SCC denied leave to appeal). In *Spasic*, the defendant brought a motion to strike certain paragraphs of the plaintiff's statement of claim on the basis that they disclosed no reasonable cause of action. The Motions Judge granted the motion at first instance for the paragraphs regarding the claims for spoliation on the grounds that a separate cause of action for spoliation did not exist in Ontario. On appeal, the Court of Appeal held that the claims for spoliation should not be struck out and that the claims pleaded should be allowed to proceed to trial as the few Canadian cases which have considered the issue were not definitive.

229. [1998] BCJ No 724 (BC CA), 157 DLR (4th) 465 (CanLII).

Significant judicial attention has been directed towards making proactive orders intended to ensure that documents are preserved as early as possible, whether in the form of Anton Piller orders or through more conventional document preservation orders.[230] Where such orders are sought, followed and enforced, evidence may remain available, avoiding the need for consideration of spoliation altogether.

Comment 11.b. Sanctions for Spoliation and Nondisclosure

Canadian jurisprudence regarding the appropriate response to a party's failure to comply with its document discovery obligations is limited but developing.[231] Courts have a wide discretion to impose suitable sanctions proportionate to the nature of the nondisclosure and its relative seriousness in the particular context.

While remedies for spoliation are generally considered at trial, pretrial relief for spoliation may be available in the exceptional case where a party is particularly disadvantaged by the destruction of evidence. Generally, where pretrial relief is awarded, the facts show either intentional conduct or indicate that a litigant or the administration of justice will be prejudiced

230. *CIBC World Markets Inc. v. Genuity Capital Markets*, 2005 CanLII 3944 (ON SC); *Canadian Derivatives Clearing Corp. v. EFA Software Services Ltd.*, 2001 ABQB 425 (CanLII); *Portus Alternative Asset Management Inc. (Re)* (2005), 28 OSC Bull 2670; *XY LLC v. Canadian Topsires Selection Inc.*, 2013 BCSC 780 (CanLII) and *Teledyne Dalsa, Inc. v. BinQiao Li*, 2014 ONSC 323 (CanLII).

231. Note that there is considerable U.S. jurisprudence on the issue of sanctions for spoliation; however, US jurisprudence should be considered only persuasive, given the significant differences in rules of court including cost consequences for nondisclosure and spoliation.

in the preparation of the case for trial.[232] Courts have awarded pretrial relief for spoliation through the applicable rules of court, or the Court's general discretion with respect to costs and the control of abuse of process.[233]

Courts may make such orders as are necessary to sanction parties appropriately for nondisclosure, particularly the intentional or reckless destruction of ESI. Canadian courts have shown a willingness to order production of documents, including ESI,[234] with sanctions following a party's noncompliance with such an order. Generally, deficiencies in disclosure have been reflected in an award of costs (whether for the other party's out-of-pocket expenses or wasted costs)[235] or the drawing of an adverse inference.[236] Other conditions may be imposed, including restrictions on the use of records subsequently located.[237] Other possible direct remedies include punitive monetary awards, jury instructions by the judge, exclusion of testimony or exhibits, findings of liability and case dismissal. Absent bad faith or significant prejudice, however, the consensus of the

---

232. *Cheung v. Toyota*, 2003 CanLII 9439 (ON SC); *Western Tank & Lining Ltd. v. Skrobutan*, 2006 MBQB 205 (CanLII).

233. *McDougall v. Black & Decker Canada Inc*., 2008 ABCA 353 (CanLII) at para 29; see also *Chow-Hidasi v. Hidasi*, 2013 BCCA 73 (CanLII), which confirms that spoliation requires intentional conduct (with "intentional" defined as "knowledge that the evidence would be required for litigation purposes" at para 29).

234. See e.g. *Spar Aerospace Limited v. Aerowerks Engineering Inc.*, 2007 ABQB 543 (CanLII), in which the Court ordered production of a party's hard drives.

235. *Farro v. Nutone Electrical Ltd.* (1990), 72 OR (2d) 637 (CanLII) (CA); *Endean v. Canadian Red Cross Society*, 1998 BCJ No 724, 157 DLR (4th) 465 (CanLII) (BCCA).

236. *Logan*, *supra* note 125.

237. *Jay v. DHL*, 2009 PECA 2 (CanLII).

Working Group is that striking a pleading may be too harsh in most circumstances.

The factors for determining the appropriate sanction for failure to comply with the obligation to disclose documents (or for other similar failures) were considered in *Zelenski v. Jamz*.[238] The Court held it was appropriate to take into account such factors as: 1) the quantity and quality of the abusive acts; 2) whether the abusive acts flow from neglect or intent; 3) prejudice, in particular with respect to the impact of the abuse on the opposing party's ability to prosecute or defend the action; 4) the merits of the abusive party's claim or defence; 5) the availability of sanctions short of dismissal that will address past prejudice to the opposing party; and 6) the likelihood that a sanction short of dismissal will end the abusive behaviour.

In *Brandon Heating and Plumbing (1972) Ltd. et al v. Max Systems Inc.*,[239] the plaintiff provided undertakings to preserve certain hardware, disks and documents as they were key to the defendant's defense. Instead, however, the hardware and software were replaced as part of the normal replacement cycle, making the evidence unavailable. The Court concluded the destruction was a willful act and the resulting prejudice was sufficient to lead to the dismissal of the plaintiff's case.

Comment 11.c. Rebutting the Presumption of Spoliation

Unlike in the United States, where Rule 37(f) of the Federal Rules of Civil Procedure (FRCP) provides for a formal "safe harbor" for the routine, good-faith operation of an electronic information system which results in the destruction or deletion of

238. *Zelenski v. Zelenski*, 2004 MBQB 256, 189 Man.R. (2d) 151 (CanLII).

239. 2006 MBQB 90, 202 Man R (2d) 278 (CanLII).

electronic evidence,[240] no formal exemption or defense against spoliation exists in Canadian court rules. The Canadian common law jurisprudence, however, reveals that courts make inquiries into the circumstance in which evidence becomes unavailable, and parties that can show that evidence became unavailable under reasonable circumstances may be able to rebut the presumptions which favour sanctions.[241]

Where a responding party asserts that a record no longer exists, a court may make an inquiry into the records management practices and policies of that party. For example, in *HMQ (Ontario) v. Rothmans Inc.*, Master Short stated that the document retention policies were relevant to the issues on the motion, and "[t]o the extent that such a policy would suggest whether, at any particular time period, a specific type of document, would or

240. Rule 37(e) provides that, absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide ESI lost as a result of the routine, good-faith operation of an electronic information system. It responds to the routine modification, overwriting and deletion of information from the normal use of electronic information systems and is intended to capture the alteration or overwriting of information that takes place without the operator's specific direction or awareness. US jurisprudence, however, suggests that the protections of FRCP Rule 37(e) applies only to information lost due to the routine operation of an information system, and only if such operation was in good faith: "The good faith requirement of Rule 37(f) [later renumbered to 37(e)] means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve." Committee Notes on Rules—2006 Amendment, online: <http://www.law.cornell.edu/rules/frcp/rule_37>. A revised Rule 37(e) ("Failure to Preserve Electronically Stored Information" [with a proposed heading in which "Preserve" replaces "Provide"] has been approved by the United States Judicial Conference and is pending Supreme Court Review as of the time of this publication.)

241. *Leon v. Toronto Transit Commission*, 2014 ONSC 1600 (CanLII) and *Stilwell v. World Kitchen Inc.*, 2013 ONSC 3354 (CanLII).

would not have been retained (and for how long) is helpful."[242] It is generally settled in Canada that records disposal under a reasonable records management policy, made in the usual and ordinary course of business, in compliance with regulatory and statutory requirements and in the absence of a legal hold, is valid and will rebut an inference of spoliation.[243] In contrast, courts have been willing to draw adverse inferences in circumstances where litigants have failed to produce relevant records and no retention policy exists,[244] and where a failure to produce a document is tied to the destruction of a document through an ad hoc procedure.[245]

Similarly, if an organization has an information governance or records management policy for retaining documents but does not follow its own policy and destroys relevant documents inconsistently with that policy, further discovery is appropriate both on the merits and to determine whether spoliation has occurred.[246]

---

242. *HMQ (Ontario) v. Rothmans Inc.*, 2011 ONSC 1083 (CanLII) at para 92.

243. *Stevens v. Toronto Police Services Board*, 2003 CanLII 25453 (ON SC). See also *Moutsios c Bank of Nova Scotia*, [2011] QJ No 1014 at para 19, 2011 QCCS 496 (CanLII) (Madame Justice Picard), in which the Court held that the bank's policy of disposing of all closed and inactive documents after six years was reasonable. To require the bank to retain guaranteed investment certificates to prove payment of these certificates would force the bank to retain its documents *ad infinitum* and that was unreasonable.

244. *Fareed v. Wood,* 2005 CanLII 22134 (ON SC); *Sunderji v. Alterna Savings*, 2010 ONSC 1223 (CanLII).

245. *Moezzam Saeed Alvi v. YM Inc.* (2003) OJ No 3467, [2003] OTC 799 (ON SC) (CanLII); *Ontario v. Johnson Controls Ltd*. (2002) OJ No 4725, [2002] OTC 950 (CanLII) (ON SC).

246. *Apotex Inc. v. H. Lundbeck A/S*, [2011] FC 88, 91 CPR (4th) 274 (CanLII).

Canadian courts have not as yet addressed the issue of parties having document retention policies with deliberately-set short retention periods after which documents are destroyed, so that destruction will happen as a matter of course before any obligation to preserve has arisen. If a policy is designed to defeat the ability of claimants to obtain evidence where the destroying party knew the destroyed documents could be relevant, however, a court may be inclined to fashion appropriate sanctions or remedies.

Finally, in some instances, parties have digitized records and can no longer produce the paper originals. The digitization of records will generally not be sufficient to ground a presumption of spoliation. For the purpose of determining admissibility of digitized electronic records in lieu of paper originals, some jurisdictions permit evidence to be presented regarding standards and best practices used by organizations and applied to the creation and storage of the digitized records.[247]

---

247. See *Canada Evidence Act*, RSC 1985, c C-5, s. 31.2; Alberta *Evidence Act*, RSA 2000, c A-18 s. 41.4; Saskatchewan *Evidence Act*, SS 2006, c E-11.2, s. 56; Manitoba *Evidence Act*, CCSM c E150, s. 51.3; Ontario *Evidence Act*, RSO 1990, c E.23, 34.1(5.1); Nova Scotia *Evidence Act*, RSNS 1989, c 154, s. 23D; An *Act to Establish a Legal Framework for Information Technology*, CQLR c C-1.1, s. 6.; and see reference to section 23(F) of the *Evidence Act*, RNS, 1989, c 154 by *Saturley v CIBC World Markets Inc.*, [2012] NSJ No 313, 2012 NSSC 226, 317 NSR (2d) 388, 2012 NSSC 226 (WL). These standards are not mandatory. Some common standards in use by organizations include: the Canadian General Standards Board, online: Public Works and Government Services Canada <http://www.tpsgc-pwgsc.gc.ca/ongc-cgsb/index-eng.html>; Standards Council of Canada, CAN/CGSB 72.34-2005 Electronic Records as Documentary Evidence, online: Standards Council of Canada <http://www.scc.ca/en/standardsdb/standards/22952>; Standards Council of Canada, Micrographics and Electronic Images as Documentary Evidence (CAN/CGSB-72.11-93 as amended 2000); International Organization for Standardization

The costs of identifying potentially relevant ESI can, in many cases, be reduced in circumstances where an organization has a well-designed and implemented information governance and records management policy ("Information Governance Policy"). Such a policy can serve as a guide in identifying the type, nature and location of information (including ESI) that is relevant to the legal proceeding as well as the potential sources of data. An Information Governance Policy could also include:

- information about an organization's information governance structure as reflected in a data map;[248]
- guidelines for the routine retention and destruction of ESI as well as paper, and for necessary modifications to those guidelines in the event of litigation;
- processes for the implementation of legal holds, including measures to validate compliance;

(ISO), ISO/CD 15489-1 Information and Documentation Records Management, Part 1 and Part 2, online: ISO <http://www.iso.org/>; Guidelines ISO/TR15489-2, online: ISO <http://www.iso.org/>; and ARMA International's Generally Accepted Recordkeeping Principles® (The Principles®), online: ARMA <http://www.arma.org>.

248. A data map is a visual reproduction of the ways that ESI moves throughout an organization, from the point it is created to its ultimate destruction as part of the organization's information governance and document retention program. Data maps address how people within the organization communicate with one another and with others outside the organization. A comprehensive data map provides legal and IT departments with a guide to the employees, processes, technology, types of data and business areas, along with the physical and virtual locations of data throughout the organization. It includes information about data retention policies and enterprise content management programs and identifies servers that contain data for various departments or functional areas within the organization.

- processes for auditing IT practices to control data proliferation (redundant backups, use of links to documents rather than attachments, etc.) and to institutionalize other good record-keeping practices; and
- guidelines on the use of social media in the business context.

It should also be noted, however, that in cases involving allegations of fraud, conspiracy, misappropriation of funds or unlawful disclosure of confidential information, the relevant ESI (which would likely include the metadata) may include records beyond the category of business records listed in the Information Governance Policy. Thus, while an Information Governance Policy should be consulted at the identification and preservation stages of e-discovery, the examination and consideration of such a policy should not limit the level of inquiry to only those types of records listed in the Information Governance Policy.

Effective information governance and records management policies will enable the parties to present a more accurate picture of the cost and burden to the Court when refusing further discovery requests, or when applying for orders shifting costs to the receiving party in appropriate cases. A detailed discussion of information governance and records retention policies is beyond the scope of this paper. Readers are encouraged to consult The Sedona Conference's *Commentary on Information Governance.*[249]

249. The Sedona Conference, *Commentary on Information Governance* (December 2013), online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/3421>.

Principle 12. The reasonable costs of all phases of discovery of electronically stored information should generally be borne by the party producing it. In limited circumstances, it may be appropriate for the parties to arrive at a different allocation of costs on an interim basis, by either agreement or court order.

In most Canadian provinces and territories, the costs of discovery are traditionally borne by the producing party and any shifting of costs to the receiving party typically occurs at the end of the litigation, at which time an unsuccessful receiving party may be required to contribute, in whole or in part, towards the costs (fees and disbursements) of the successful party.[250] This generally includes allocation of the costs of producing ESI. This can be contrasted with the practice when paper

250. See e.g. Supreme Court of British Columbia, *Practice Direction Re: Electronic Evidence* (July 2006) at s 3.1, online: The Courts of British Columbia <http://www.courts.gov.bc.ca/supreme_court/practice_and_procedure/electronic_evidence_project.aspx>. The Practice Direction provides that the reasonable costs of complying with the Practice Direction, "including the expenses of retaining or utilizing necessary external or in-house technical consultants," may be claimed as costs under the *Rules of Court*. See also *Doucet v. Spielo Manufacturing Inc*., 2012 NBQB 324 (WL). At issue was an assessment of the defendant's Bill of Costs following completion of a trial and appeal. Prior to trial, a document production order had been made requiring the defendants to provide the plaintiff with access to their computer system. The Motions Judge was aware, when the order was made, of the potential cost and extent of the operation. An amount of $40,000 was the estimated cost stated at the motion hearing. The final cost was $22,926.81. Despite the plaintiff's argument that the defendants could have fulfilled the order through a more economical method, the Registrar awarded the defendants the full costs of the computer consultant's report. While the defendants were the producing party, and therefore incurred the costs arising during the pretrial phase, the defendants were ultimately successful at trial and therefore entitled to reimbursement of these costs by the plaintiff, in accordance with the

documents are produced where the receiving party has traditionally been responsible for the immediate costs of the production, such as copying, binding and delivery costs.

While litigants are properly expected to bear the costs, on at least an interim basis, of producing ESI in the ordinary course, different considerations are engaged when extraordinary effort or resources will be required to first restore data to an accessible format (e.g. accessing disaster recovery tapes, residual data or data from legacy systems). In such cases, if the data is producible at all, requiring the producing party to fund the significant costs associated with restoring such data may be unfair, and may hinder the party's ability to litigate the dispute on the merits. Accordingly, it may be appropriate that the party requesting such extraordinary efforts should bear, at least on an interim basis, all or part of the costs of doing so. Parties are encouraged to consider these issues when they negotiate a discovery plan.[251]

In Canada, a court is empowered to order that the costs of producing accessible ESI be shifted in certain circumstances.[252] In deciding whether to make an order on an interim

---

traditional approach to discovery costs. See also *Bank of Montreal v. 3D Properties,* [1993] SJ No 279 at para 30, 111 Sask. R 53 (WL) (QB): "All reasonable costs incurred by the plaintiff, including *inter alia*, searching for, locating, editing and producing said 'documents': computer records, discs and/or tapes for the applicant shall be at the applicant's cost and expense."

251. See Supreme Court of British Columbia, *Practice Direction Re: Electronic Evidence* (July 2006) at s 6 online: The Courts of British Columbia <http://www.courts.gov.bc.ca/supreme_court/practice_and_procedure/electronic_evidence_project.aspx>, which recommends that parties consider the issue of transferring the costs of the search for, and the discovery of, ESI.

252. See e.g. *Warman v. National Post Company*, 2010 ONSC 3670 (CanLII), in which the Master held that the costs of the expert who would conduct a forensic examination of a limited subset of the data on the plaintiff's hard drive would be paid initially by the defendant seeking production of the

basis shifting the costs of production of electronically stored information, the Working Group recommends that a court consider the following factors:

1. whether the information is reasonably accessible as a technical matter without undue burden or cost;
2. the extent to which the request is specifically tailored to discover relevant information;
3. the likelihood of finding information that is important and useful;
4. the availability of such information from other sources, including testimony, requests for admission and third parties;
5. the producing party's failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessible sources, and the reasons for that lack of availability;
6. the total cost of production (including the estimated costs of processing and reviewing retrieved documents), compared to the amount in controversy;
7. the total cost of production (including the estimated costs of processing and reviewing retrieved documents), compared to the resources available to each party;

---

drive, with the ultimate responsibility for that expense being in the discretion of the Trial Judge. In addition, in *Borst v. Zilli*, 2009 CanLII 55302 (ONSC), the Court found that the plaintiffs' request to conduct an inspection of the defendant's electronic data was similar to a request to inspect property under Rule 32 of the Ontario *Rules of Civil Procedure*. The costs of such inspection by an independent computer consultant were therefore to be borne by the plaintiffs. The Court did order that the costs of an independent solicitor to review the documents for privilege and relevance were to be shared by the parties given that such review could have been done by defendant's counsel but the plaintiff refused that option.

8. other burdens placed on the producing party, including disruption to the organization, lost employee time and other opportunity costs;
9. the relative ability of each party to control costs and its incentive to do so;
10. the importance of the issues at stake in the litigation; and
11. the relative benefits to the parties of obtaining the information.[253]

Courts still often continue to follow the traditional rule and refuse to shift the costs of production of ESI at the discovery stage. In *Gamble v. MGI Securities*,[254] the Court ordered the defendant to deliver its productions in CSV format and refused to shift the costs of doing so to the plaintiff. In doing so, the Court took into account The Sedona Canada Principle 12 and the disparity in the parties' abilities to pay for production. Similarly, in *GRI Simulations Inc. v. Oceaneering International Inc.*,[255] the Court found no reason to depart from the traditional approach to costs at the production stage. Costs were therefore to be borne by the producing party.

E-discovery may involve significant internal client costs as well as counsel fees and disbursements for outsourced services. There may be a need for the cost rules to be clarified so that internal discovery costs are regarded as a recoverable disbursement in appropriate cases. Disbursements made to a third party or billed to a client for electronic document management

253. See the discovery plan and proportionality rules under the *Ontario Rules*, *supra* note 10 (Rules 29.1 and 29.2); [U.S.] Federal Rules of Civil Procedure 26(b)(2)(B); *U.S. Sedona Principles*, *supra* note 222, Comment 13.a.

254. *Gamble v. MGI Securities*, 2011 ONSC 2705 (CanLII).

255. *GRI Simulations Inc. v. Oceaneering International Inc.*, 2010 NLTD 85 (CanLII). See also *Veillette v. Piazza Family Trust*, 2012 ONSC 5414 (CanLII).

should now be considered a standard disbursement.[256] These costs could also, therefore, be subject to a cost-shifting order.

As e-discovery costs may be significant and given that cost shifting occurs relatively infrequently, parties should adopt strategies to control the costs of e-discovery. Good Information Governance policies and practices are the most proactive method of reducing costs associated with e-discovery and maintaining proportionality in the discovery process.[257] Given the potential for an interim cost award in an e-discovery context, a party seeking production of electronic documents should also carefully consider the cost implications as early as possible.[258] A producing party may wish to limit the scope of its e-discovery obligations, through negotiation, appropriate admissions or motions. It may also wish to consider whether the costs should be partially or completely shifted to the receiving party.[259]

---

256. See *Harris v. Leikin Group*, 2011 ONSC 5474 (CanLII).

257. The Sedona Conference, *Commentary on Information Governance* (December 2013), *supra* note 249.

258. Some Canadian jurisdictions have practice directions in place for managing electronic evidence, including cost benchmarking. See e.g. Supreme Court of British Columbia, *Practice Direction Re: Electronic Evidence* (July 2006), online: The Courts of British Columbia <http://www.courts.gov.bc.ca/supreme_court/practice_and_procedure/electronic_evidence_project.aspx>; Sandra Potter, *Guidelines on Benchmarking of Costs*, online: Canadian Judicial Council <https://www.cjc-ccm.gc.ca/english/news_en.asp?selMenu=news_publications_en.asp>.

259. *Barker v. Barker*, 2007 CanLII 13700 (ONSC). The defendants moved for orders requiring the plaintiffs to pay one-third of the cost of scanning and coding the documents; the other two-thirds to be borne equally by the Crown and the defendant physicians. The motions were opposed by the plaintiffs. The Court agreed that the benefits to the plaintiffs justified an order for the sharing of the costs of conversion.

Shifting the costs of extraordinary discovery efforts, however, should not be used as an alternative to making a well-founded objection to undertaking such efforts in the first place. Extraordinary discovery efforts and any associated cost shifting should be required only where the requesting party demonstrates substantial need or justification. The courts should discourage burdensome requests that have no reasonable prospect of significantly contributing to the discovery effort, even if the requesting party is willing to pay.