The Sedona Conference Journal

Volume 23 2022

The Sedona Canada Principles Addressing Electronic Discovery, Third Edition

The Sedona Conference

Recommended Citation:

The Sedona Conference, *The Sedona Canada Principles Addressing Electronic Discovery, Third Edition*, 23 SEDONA CONF. J. 161 (2022).

For this and additional publications see: https://thesedonaconference.org/publications.

THE SEDONA CANADA PRINCIPLES
ADDRESSING ELECTRONIC DISCOVERY, THIRD EDITION

A Project of The Sedona Conference Working Group 7 (Sedona Canada)

Author:

The Sedona Conference

Editorial Team:

Nicholas Trottier
David Outerbridge
Susan Wortzman
Kathryn Manning

Drafting Team:

Carolyn Anger
Rachael Chadwick
Pamela Drummond
Maura Grossman
Shoshana Israel
Kristen Lai
Sarah Millar
Chuck Rothman
Anatoliy Vlasov
Stephanie Williams
Gretel Best
Lyndsey Delamont
Lauren Fishman
Scott Hunter
Rachael Jastrzembski
Michael Lalande
Suzan Mitchell-Scott
Tiana Van Dyk
Dawn Sullivan Willoughby

Staff editor:

David Lumia

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

This publication may be cited as follows:

> The Sedona Conference, *The Sedona Canada Principles Addressing Electronic Discovery, Third Edition,* 23 SEDONA CONF. J. 161 (2022).

PREFACE

Welcome to the Third Edition of *The Sedona Canada Principles Addressing Electronic Discovery* (the *"Principles"*), a project of The Sedona Conference Working Group 7 on eDiscovery Issues in Canada ("Sedona Canada" or "WG7"). This is one of a series of Working Group commentaries published by The Sedona Conference, a nonprofit, nonpartisan research and educational organization 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, intellectual property rights, and data security and privacy law, 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 the *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 of the *Principles* was published in November 2015. Since that time, there have been significant technological and societal changes that have changed how we manage eDiscovery. We have done our best to reflect those changes in this *Third Edition*. The endorsement of the *Principles* by the courts in several jurisdictions and their recognition in provincial rules of procedure created a responsibility that the drafters of this *Third Edition* have taken seriously. As a result, the drafting team and editors carefully considered all the changes that have

been made and the impact they may have on the litigation process.

On behalf of The Sedona Conference, I thank Editorial Team leaders Nicholas Trottier, Susan Wortzman, David Outerbridge, and Kathryn Manning and all members of the Drafting Team for their time and attention during the drafting and editing process: Carolyn Anger, Gretel Best, Rachael Chadwick, Lyndsey Delamont, Pamela Drummond, Lauren Fishman, Maura Grossman, Scott Hunter, Shoshana Israel, Rachael Jastrzembski, Kristen Lai, Michael Lalande, Sarah Millar, Suzan Mitchell-Scott, Chuck Rothman, Tiana Van Dyk, Anatoliy Vlasov, Dawn Sullivan Willoughby, and Stephanie Williams. I also wish to acknowledge Charles Boocock for his involvement, as well as several others who made special contributions to this *Third Edition*. Thank you for the updates and advice relating to privacy law from Molly Reynolds, Nic Wall, and Ronak Shah. Thanks to Chuck Rothman, who did a full review of the updated technology comments. A special thanks to Jared Toll, who spent hours updating and correcting the footnotes for this edition.

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 Weinlein
Executive Director
The Sedona Conference
January 2022

TABLE OF CONTENTS

I. INTRODUCTION

In 2008, when the First Edition of the *Sedona Canada Principles* was released, it included a lengthy Introduction explaining what eDiscovery was, why it was important, and why the courts and parties should be thinking about eDiscovery. In 2021, we no longer think it is necessary to explain the importance of digital evidence in the litigation process. It has really become standard process for litigants, their lawyers, and the courts, who must now consider electronic evidence in almost every matter.

The previous Introduction also included a discussion about the overarching principles that were and continue to be embodied in the *Sedona Canada Principles*. That discussion focused on Proportionality and Cooperation between parties. None of that has changed, and the best practices remain the same . . . the courts and parties should always endeavour to take a proportionate and cooperative approach when they are dealing with voluminous and complex datasets of electronically stored information (ESI). The spirit of proportionality and cooperation is also reflected in many provinces, which have mandated discovery plans or protocols. In complex matters, parties are now accustomed to agreeing to discovery protocols that govern the scope and exchange of ESI. This is good for parties, both in terms of efficiencies and cost.

In 2021, we are also facing a proliferation of new types of data. These range from ephemeral data to the chat tools that we use to communicate daily. Those new tools, compounded with a global pandemic that has kept many of us working from home, have had a profound impact on managing ESI and eDiscovery. Lawyers who went into the office six days a week are now working from home and have developed new ways in which to communicate that we never before thought were possible. Our clients' businesses and the ways that they create, manage, and use their data have changed dramatically. In the

eDiscovery arena, we now need to consider different data sources and the best ways to collect data remotely. As we practice law in this transforming world, we see that eDiscovery processes have advanced to accommodate the new ways in which we are working. The *Sedona Canada Principles*, while they remain neutral on the technology, attempt to incorporate best practices that will take into consideration this evolving digital world.

Machine learning has also been a game changer, dramatically expanding and evolving ways to process ESI and deploy artificial intelligence in doing so. This creates new challenges for eDiscovery practitioners. However, we are appreciative that the eDiscovery community had the opportunity to be an early adopter of machine learning through technology-assisted review (TAR) and continuous active learning tools that were developed to support our community. Being early adopters has created much opportunity for eDiscovery specialists. These machine learning tools and processes are also discussed in this *Third Edition*.

The transformations that we have seen have proved to be societal as well. The Editorial Committee has chosen to modify the many references to "native" records or information. We now refer to "original digital files." This change was made in response to sensitivities raised by our Indigenous community and the confusion surrounding the reference to certain records as "native" records. While we appreciate that "native records" was a term of art in the eDiscovery community, in the spirit of reconciliation that we are undergoing in Canada, the Editorial Committee thought it important to make this change to the terminology in this document.

In 2021, we are addressing the interplay between eDiscovery and developing privacy regimes in Canada, and the role of information governance to facilitate eDiscovery.

These are just a few of the many changes contained in the *Third Edition*, plus the ever-growing body of case law. In a few 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 here:

Principle 1 (ESI is discoverable): New case law and illustrations have been added in the Commentary section on Relevancy.

Principle 2 (Proportionality): Minor changes have been made to the language of the Principle, and new case law and illustrations have been added in the Commentary section on the evidentiary foundation for proportionality.

Principle 3 (Preservation): The Principle has been amended to now include anticipated investigations in the duty to preserve ESI. A new Commentary section (3.d) has been added to address investigation preservation. Additionally, a new Commentary section (3.g) has been added to cover privacy obligations, taking into consideration the various national and subnational privacy laws that may apply to the personally identifiable information (PII) being preserved.

Principle 4 (Cooperation): The Commentary has been updated to encourage parties to discuss use of technology throughout the discovery process, to consider phased or tiered discovery to allow for more time to deal with data sources that are harder to collect or process, and to encourage the spirit of collaboration and cooperation where parties are technologically unevenly matched.

Principle 5 (Duty to produce): The Commentary in this Principle has been updated to consider the role of Information Governance and Records Management in facilitating the discovery process. New case law has been added as examples of the use of

backup media to collect ESI when the requisite data is not available through standard data collection. Finally, the complex issues that arise from ESI stored in cloud-based platforms or hosted with third-party vendors are addressed.

Principle 6 (Deleted or residual data): A new paragraph on ephemeral data has been added at the end of the Commentary of this Principle.

Principle 7 (Use of technology): Considering the importance of technology and its role in reducing time and costs in eDiscovery, it should not be surprising that extensive modifications and additions have been made to the Commentary of this Principle. Parties should have a minimum understanding of the tools they use and appropriately apply technology, workflows, and expertise to arrive at a defensible process. Despite all the technological tools available to counsel to facilitate the eDiscovery process, keyword searches are still commonly used. A new list of pros and cons has been added to the Commentary to address the challenges and limitations of relying on keyword searches.

Principle 8 (Discovery planning): The Principle has been amended to focus on the scope rather than the substantive content of production. New Commentary sections have been added to encourage parties to agree on the scope of production (8.c) and to address the positive obligation to assist an opposing party to better manage and understand large document productions (8.e).

Principle 9 (Privilege and confidentiality): The Commentary sections have been updated to persuade parties not to rely only on keyword searches to identify privileged or confidential information, and to encourage more innovative approaches, including using more technology such as TAR and better redaction tools. The privacy section has been updated with new case law related to social media, the General Data Protection

Regulation (GDPR) that came into force in the European Union in 2018, and references to *The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers*. A new section on privacy and ephemeral messaging (9.c.ii) has been added. Finally, the data security section (9.d) has been updated with references to *The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers*.

Principle 10 (Multijurisdictional eDiscovery): The Commentary has been updated to better nuance the differences between provinces and other jurisdictions, and the issues arising from multijurisdictional litigation. The Commentaries on privacy and confidentiality have been updated to address data transfer prohibitions from certain jurisdictions such as the European Union due to GDPR. Additional guidance is given to address differences in protection of certain categories of privilege varying from jurisdiction to jurisdiction. For cross-border cases, parties are reminded that the collection, review, and production of data in one forum could have an impact on the disclosure of evidence in another. Finally, the arbitration section of the Commentary has been updated with many useful references to the ADR Institute of Canada (ADRIC) Arbitration Rules.

Principle 11 (Sanctions): The language of the Principle has been softened: "Sanctions should be considered by the Court" was changed to "Sanctions may be appropriate". The Commen-tary of this Principle went from three sections to six sections. New sections have been added to consider the existence of a tort of spoliation in Canada and address the negligent destruction of evidence. Finally, a new case law analysis of the various rem-edies granted by the courts was added.

Principle 12 (Cost): The Commentary has been updated to reflect the rising costs and potential liabilities associated with the discovery of ESI. The increased use in technology due to world events like COVID-19 has created an explosion of digital

information, and the costs of eDiscovery will also increase due to the magnitude of digital information. The decisions made regarding eDiscovery processes and workflows can have significant impact on costs. The Commentary has now been segregated into two sections to reflect the different phases of discovery and what type of actions/inactions will attract cost awards. The Commentary of this Principle has also been updated with various recent case law decisions.

Kathryn Manning
David Outerbridge
Nicholas Trottier
Susan Wortzman

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 electronically stored information (ESI) must be produced as part of the discovery process. Typical forms of ESI include, but are not limited to, email data, word-processing files, spreadsheets, web pages, video and sound recordings, chat and text messages, digital photographs, information on web pages and social media, mobile device data, structured data, the Internet of Things,[1] location data, and biometric data.[2]

The *Personal Information Protection and Electronic Documents Act*[3] 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

1. The Internet of Things is a catchall term used to describe a broad array of electronic devices, such as computers or sensors in cars, refrigerators, lights, or security systems, that are connected to the internet and may collect, store, and/or share information, see "The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition," (2020) 21 Sedona Conf J 263 at 325 ["Sedona Conference Glossary"].

2. Biometric data is personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data, see *ibid* at 274.

3. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5. [*PIPEDA*].

computer system or other similar device. It includes a display, printout or other output of that data." The *Canada Evidence Act*[4] 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."

Québec passed An Act to Establish a Legal Framework For Information Technology,[5] which includes the following definition:

> "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.[6] Rules of court make relevancy a

---

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

5. [*Québec Information Technology Act*], CQLR c C-1.1, s 3.

6. See, e.g., *Cholakis v Cholakis*, 2000 CanLII 20735 (MB QB) at para 30 [*Cholakis*]:

"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."

prerequisite to production, regardless of the form of record. For example, Part Five, Rule 5.2(1) of the *Alberta Rules of Court*[7] provides that producible records be both relevant and material. The Ontario *Rules of Civil Procedure*[8] provide that every document relevant to any matter in question in the action shall be produced. The British Columbia rules were amended in 2009 to introduce concepts of proportionality and narrow the scope of documentary discovery.[9]

Courts have ordered the production of actual media in particular cases, such as in *Reichmann v. Toronto Life Publishing Co.*,[10] 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.*,[11] 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

7. *Alberta Rules of Court*, r 5.2(1)

8. Ontario *Rules of Civil Procedure,* 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.

9. *Supreme Court Civil Rules*, rr 1-3(2), 7-1(1)

10. *Reichmann v Toronto Life Publishing Co*., 1988 CanLII 4644 (ON SC).

11. *Northwest Mettech Corp. v Metcon Service Ltd*., 1996 CanLII 1056 at para 10 (BC SC).

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.[12] This suggests that access for forensic purposes such as recovering deleted information may be permitted.

In *JEP v. ECB,*[13] a negative inference regarding credibility was made against the respondent in the proceedings due in part to a failure to produce Facebook chat message records in connection with a matrimonial dispute. The Court determined that "He also failed, despite being requested to do so, to produce any records of Facebook messages between him and R.J. after June of 2016. Given the nature and tone of the exchanges with R.J. and the failure to disclose the requested records, I do not believe the respondent's denials."

In *Hodgson v. Coast Storage and Containers Ltd.*,[14] the Tribunal did not take issue with the defendant filing a series of Microsoft Teams chat messages in support of its position. While the plaintiff submitted that the Microsoft Teams messages should not be weighed since they were not "adequately contextualized" or sworn as part of an affidavit, the Tribunal concluded, "Although the evidence is not in a sworn format, that does not, in my view, detract from its value . . . ."

> *Illustration i—Discovery of ESI over Paper Documents*: A claim is commenced against a business owner by a former supplier for breach of contract. The statement of claim alleges that the business owner failed to pay

12. *Nicolardi v Daley*, [2002] OJ No 595 at para 5 (ON SC).

13. *JEP v ECB*, 2019 BCSC 786 (CanLII) at para 86.

14. *Hodgson v Coast Storage and Containers Ltd.,* 2020 BCHRT 55 para 57 [*Hodgson*].

the supplier for goods and services rendered for the preceding 24 months in excess of $300,000.

As part of the business owner's production obligation, his lawyer asks him to collect all email communications between him and the supplier along with all invoices and financial documents that were submitted to the business owner by the supplier in original electronic format. The business owner has some printed hard copies of emails, invoices, and invoice summary spreadsheets received from the supplier, but not all. The business owner must ensure that he preserves, collects, and produces original digital emails, electronic invoices, and spreadsheets rather than providing his lawyer with an incomplete set of printed hard-copy versions of the documents.

Illustration ii—Discovery of ESI Metadata Required by Both Parties: An asset management company (ABC Asset Management) sues a former principal for breach of fiduciary duty, breach of contract, and breach of trust. The former principal of ABC resigned and started her own investment banking firm. The new business is in direct competition with ABC. ABC discovers that shortly after her resignation, the former principal solicited existing and potential clients of ABC via email and made and retained copies of agreements, stock research and analysis, and confidential work product created and owned by ABC.

The former principal should ensure that she preserves, collects, and produces all electronic documents in her possession with all associated metadata intact evidencing the author, creation, and modification dates of the agreements, stock research and

analysis, and confidential work product allegedly created and owned by ABC.

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.[15] 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.

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

15. 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 Northwest 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.Québec's legislation is the *Québec Information Technology Act*.

related to the admissibility of records, except the rules relating to authentication and best evidence.[16]

Principle 2. **In any proceeding, steps taken in the discovery process should be 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 ESI; (iv) the importance of the ESI to the court's adjudication in a given case; and (v) the costs, burden, and delay that the discovery of the ESI 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.[17] 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.

16. See, e.g., *Evidence Act*, RSO 1990 c E.23, s 34.1; *Québec Information Technology Act*; s 5, 6 and 7.

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

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 norm. Master Short's decision in *Siemens Canada Limited v. Sapient Canada Inc*.[18] provides an important analysis of proportionality and expectations of counsel to comply with this principle.[19] This decision provides guidance for discovery planning and the transparency required by counsel in meeting their obligations.[20]

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

---

18. *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 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.

19. See also detailed analyses in: *Warman v National Post Co* 2010 ONSC 3670 (CanLII); *Kaladjian v Jose*, 2012 BCSC 357 (CanLII) [*Kaladjian*]; The Sedona Conference, "The Sedona Canada Commentary on Proportionality in Electronic Disclosure & Disclosure" (Oct. 2010 public comment version) and its Appendix 1, online: The Sedona Conference <https://thesedonaconference.org/publication/The_Sedona_Canada_Commentary_on_Proportionality_in_Electronic_Disclosure_and_Discovery>.

20. *Siemens*, *supra* note 18; *Hryniak v Mauldin*, 2014 SCC 7 (CanLII) [*Hryniak*]; see also <https://canliiconnects.org/en/summaries/27537> for a discussion on the key points of *Siemens*.

are often used by a party seeking to reduce disclosure obligations, sometimes appropriately and sometimes inappropriately.

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. Parties should take a practical and efficient approach to electronic discovery and 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 ha[ve] become necessary . . . ."[21]

The case law underscores that "proportionality is a parsimonious principle."[22] 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 eDiscovery process from the outset with a view to analyzing the potential costs of eDiscovery, the means of controlling such costs, and the process that might best achieve proportionality.[23] As stated by the Court in

---

21. *Kaladjian*, *supra* note 19; *Szeto v Dwyer*, 2010 NLCA 36 (CanLII) [*Szeto*]; citing N. Smith J in *More Marine Ltd. v Shearwater Marine Ltd*., 2011 BCSC 166 (CanLII).

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

23. *L'Abbé v Allen-Vanguard*, 2011 ONSC 7575 (CanLII) at para 24 [*L'Abbé*]: "efficiency and cost effectiveness in production and discovery should be a mutual goal. Questions of relevance and privilege must be answered of

Siemens: "Now 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."[24]

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. Nonmonetary 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 (IT) 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.[25] In the discovery context, Canadian courts emphasize their mandate to meet that objective.[26] Courts have declined to order production of documents where the parties have demonstrated that the costs of producing documents or the adverse effect upon other interests, such as privacy and

---

course but it is necessary to apply those filters in a practical manner . . . Equally or more important is the need for collaborative and creative goal oriented problem solving by the parties and their respective counsel."

24. *Siemens*, *supra* note 18 at para 51.

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

26. *L'Abbé*, *supra* note 23 at para 41.

confidentiality, outweigh the likely probative value of the documents.[27]

It has also been suggested that discovery disputes need to be proportionate and not themselves be an occasion for adversarial advocacy. Alternate forms of adjudication for discovery disputes, such as a reference under Ontario's Rule 54.03, may be appropriate.[28] At least one judge of the Ontario Superior Court of Justice included proportionate electronic discovery and planning in his standard Case Management Directions.[29] Proportionality applies not only to the parties' use of their own resources, but also to their use of the court's time.[30]

Comment 2.b. The Proportionality Rule by Jurisdiction

Most Canadian jurisdictions have amended their respective rules of court to expressly include proportionality as a general rule for discovery procedures.

---

27. *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) [*Ireland*] (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 (CanLII) [*Janzen*] (declining to order production of hard drive in the particular circumstances of the case); *Desgagne v Yuen,* 2006 BCSC 955 (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.).

28. *Siemens*, *supra* note 18 at para 40; *Lecompte Electric Inc. v Doran (Residential) Contractors Ltd.,* 2010 ONSC 6290 (CanLII) at para 15.

29. *Yan v Chen,* 2014 ONSC 3111 at Appendix A (CanLII).

30. *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.").

The Chief Justice of the Supreme Court of British Columbia promulgated a *Practice Direction Regarding Electronic Evidence* (effective July 1, 2006),[31] 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 of the Practice Direction 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.[32]

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*,[33] the Court observed: "there is a discretion to limit discovery where it would be just to do so, such as where the burdens that would be placed upon the party making answer clearly outweigh the interests of the party questioning."

In Québec, section 18 of the *Code of Civil Procedure* (CCP) reads as follows: "The parties to a proceeding must observe the principle of proportionality and ensure that their actions, their pleadings, including their choice of an oral or written defence, and the means of proof they use are proportionate, in terms of

---

31. Courts of British Columbia, *Practice Direction Re: Electronic Evidence* (2006), online: Courts of British Columbia <https://www.bccourts.ca/supreme_court/practice_and_procedure/practice_directions_and_notices/electronic_evidence_project/Electronic%20Evidence%20July%201%202006.pdf>.

32. *Ibid*.

33. *Nova Scotia (Attorney General) v Royal & Sun Alliance Insurance Co. of Canada*, 2003 NSSC 227 (CanLII) at para 8.

the cost and time involved, to the nature and complexity of the matter and the purpose of the application. Judges must likewise observe the principle of proportionality in managing the proceedings they are assigned, regardless of the stage at which they intervene. They must ensure that the measures and acts they order or authorize are in keeping with the same principle, while having regard to the proper administration of justice."[34]

Québec courts have indicated that the proportionality rule must be interpreted in conjunction with section 19 CCP.[35] Section 19 reads as follows: "Subject to the duty of the courts to ensure proper case management and the orderly conduct of proceedings, the parties control the course of their case insofar as they comply with the principles, objectives, and rules of procedure and the prescribed time limits. They must be careful to confine the case to what is necessary to resolve the dispute, and must refrain from acting with the intent to cause 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 compact disks,[36] to the examination of a witness by videoconference,[37] 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.[38] Although "Courts ensure proper case management and the orderly conduct of proceedings," according to section 19

34. *Québec Code of Civil Procedure*, s 18.

35. *9103-3647 Québec Inc. c Couët*, 2003 IIJCan 14311 (CanLII) (QC CS).

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

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

38. *Parsons c. Communimed Inc.*, 2005 CanLII 11855 (QC CQ).

CCP paragraph 1, the application of the proportionality rule relies on the parties, as stated by section 18 CCP.[39]

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.[40]

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 to support its position.[41]

In the British Columbia case *Araya v. Nevsun Resources Inc.*,[42] the plaintiff produced redacted documents from Facebook Messenger or another electronic messaging application. In response, the defendant applied for an order for the plaintiffs to deliver

---

39. 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).

40. *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).

41. *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); *Velsoft Training Materials Inc. v Global Courseware Inc*., 2011 NSSC 274 [*Velsoft*]; *Hodgson*, *supra* note 14 at para 8; *Siemens*, *supra* note 18 at paras 142–44; *Hudson v ATC Aviation Technical Consultants*, 2014 CanLII 17167 at para 13 (ON SC) [*Hudson*]; *Kaladjian*, *supra* note 19 at paras 62–64. But see *HMQ* (*Ontario) v Rothmans Inc.*, 2011 ONSC 1083 (CanLII).

42. *Araya v Nevsun Resources Inc.*, 2019 BCSC 1912 (CanLII) [*Araya*].

three unredacted versions of the produced documents. The application was granted, as the court found that the plaintiff's approach of treating each post as a separate document for purposes of production and redactions was not efficient, would increase cost and would cause delay, and was not the approach that best served the truth-seeking objective. The court concluded that Facebook messages should be viewed as single documents for this purpose and that redactions were not appropriate, as relevance alone does not justify redaction.

The Digital Evidence and eDiscovery Working Group, formerly known as the E-discovery Implementation Committee, has prepared a model chart to assist parties to argue production motions based on proportionality.[43] The case law supports the use of the chart to structure proportionality arguments.[44]

> *Illustration – proportionality:* A requesting party demands that the responding party preserve, restore, and produce ESI about a topic in dispute from an unstructured data source. The requesting party produces strong evidence that important relevant ESI, not available elsewhere, is likely to exist within that data source. The ESI is reasonably accessible but is somewhat burdensome to acquire.
>
> Satisfying the production request and the importance of the information must be balanced against the cost of obtaining the data. The responding party should preserve, restore, and produce the requested ESI, since the requesting party produced strong evidence

43. 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>.

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

> of the relevance of the data, and although the data is somewhat burdensome to obtain, it is still reasonably accessible and therefore falls within the scope of proportionality.

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 the broader role proportionality has in civil litigation. In *Hryniak v. Mauldin*,[45] 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.[46]

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. . . .
>
> 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.

45. *Hryniak*, supra note 20 at para 87.

46. *Ibid* at paras 23–33.

Noting that the proportionality principle is reflected in many of the provinces' rules of court, 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,[47] 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 a specified threshold ranging from $15,000 to $200,000, depending on the province. For example, in Manitoba, Rule 20A of the Court of Queen's Bench Rules[48] modifies ordinary litigation procedures for certain actions to require the Court to consider what is reasonable where the amount at issue warrants a summary judgment or trial. Rule 20A limits the times when actions subject to this Rule may be brought and modifies the generally broad scope of discoverable documents. In particular, "relevant document" means only those documents referred to in the party's pleading, the documents to which the party intends to refer at trial, and all documents in the party's control or possession that could be used to prove or disprove a material fact at trial.

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

---

47. *Szeto*, *supra* note 21, cited at *Hryniak*, *supra* note 20 at para 31.

48. *Manitoba Rules;* see also *Ontario Rules*, r 76 presenting a Simplified Procedure applicable to most civil actions involving less than $100,000.

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/nonspoliation of evidence, including ESI.[49]

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 an organization receives threats of litigation on a daily basis, having to preserve all data every time a letter is received would effectively mean that the organization 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, 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 in advance of a determination of whether or not to collect data. Organizations and, in particular, IT departments often maintain a data map,[50] which could be a

---

49. 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 prescribe statutory requirements for record keeping. Records management and obligations to meet regulatory and statutory record keeping are outside the scope of *The Sedona Canada Principles Addressing Electronic Discovery*.

50. Data map: A document or visual representation that records the physical or network location and format of an organization's data. Information

useful starting point for this exercise. In the absence of such, a data map can be created with the aid of an organization's IT department.

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 in advance. Information governance[51] is growing in importance beyond just the realm of eDiscovery, implicating virtually all operations of an organization. To reflect the importance of information governance and its "downstream" effects in an eDiscovery engagement, the Electronic Discovery Reference Model (EDRM)

---

about the data can include where the data is stored, physically and virtually, in what format it is stored, backup procedures in place, how the electronically stored information moves and is used throughout the organization, information about accessibility of the electronically stored information retention and lifecycle management practices and policies, and identity of records custodians. See "Sedona Conference Glossary," *supra* note 1 at 263.

51. Information Governance: The comprehensive, interdisciplinary framework of policies, procedures, and controls used by mature organizations to maximize the value of an organization's information while minimizing associated risks by incorporating the requirements of: (1) eDiscovery, (2) records and in-formation management, and (3) privacy/security, into the process of making decisions about information. See *ibid* at 322.

incorporated information governance into its diagram in 2007[52] and has also developed an Information Governance Reference Model.[53]

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 eDiscovery response team, with representation from key stakeholders, including legal, business unit leaders, IT, records/information governance, human resources, corporate security, and perhaps external eDiscovery consultants/service providers. Smaller organizations can similarly prepare for litigation by establishing and maintaining solid information governance policies.

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

---

52. EDRM, EDRM Diagram Elements, online: EDRM <https://edrm.net/resources/frameworks-and-standards/edrm-model/edrm-diagram-elements/>.

53. The Information Governance Reference Model (IGRM) is more than an expansion of this one cell in the EDRM. See EDRM, Information Governance Reference Model (IGRM), online: EDRM. "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 and various provinces. The Sedona Canada Working Group favors continuing efforts to reach consensus on principles, protocols, and best practices in information governance and eDiscovery.

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 records, and account for necessary modifications to those guidelines in the event of litigation. Data maps tracking how individuals interface with various network systems should also be created and maintained.

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 (e.g., whether the sources contain structured or unstructured data[54]) 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 records 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."[55]

---

54. Structured data is a standardized format for providing information about a page and classifying the page content, online <https://developers.google.com/search/docs/guides/intro-structured-data>.

55. *Siemens*, *supra* note 18 at paras 135–38.

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.[56] As noted above, in common law jurisdictions, the preservation obligation arises as soon as litigation is contemplated or threatened.[57] Owing to the dynamic nature of ESI, any delay increases the risk of relevant evidence being lost and

---

56. *Doust v Schatz*, 2002 SKCA 129 (CanLII) [*Doust*] at para 27:

"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 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."

57. See *Culligan Canada Ltd. v Fettes*, 2009 SKQB 343 (CanLII) (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.

subsequent claims of spoliation.[58] A proactive preservation plan will ensure a party can respond meaningfully and quickly to discovery requests or court orders.

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.[59]

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.[60] The courts have ordered

---

58. 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 (CanLII); *Spasic Estate v Imperial Tobacco Ltd., et al*, 2000 CanLII 17170 [*Spasic*]. On the issue of the appropriate relief in connection with negligent spoliation, see *McDougall v Black & Decker Canada Inc.*, 2008 ABCA 353 (CanLII) [*McDougall*].

59.Nova Scotia *Civil Procedure Rules,* r 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.

60. In contrast to the extensive case law and commentary in the United States, the law regarding preservation of electronic documents in Canada is

more targeted preservation.[61] 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. Response Regarding Investigation Preservation

In the context of an investigation, the duty to preserve documents may or may not be triggered, depending on whether the investigation relates to events or allegations that give rise to a reasonable anticipation of litigation. This is true whether the investigation is internal or external. Where the duty to preserve is triggered, organizations must take reasonable steps to preserve potentially relevant ESI.

> *Illustration i.* A corporate investigation is undertaken in relation to allegations that a senior member of the

---

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 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, 217 (S.D.N.Y. 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 (S.D.N.Y. 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."

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

executive team has been harassing one of his administrative assistants and intimating that he would fire her if she does not respond to his alleged demands. The accused executive has only been with the company for eight months and has two administrative assistants reporting to him. The first assistant started her tenure within the same time period as the executive; the second (who filed the complaint) only commenced her employment within the past two months.

The corporation actively stores live email communications and Slack chat messages for a period of six months' time before resorting to archives.

General Counsel to the corporation and the Human Resources Director formed an internal investigations team and decided to preserve all archived email and chat communications generated by the executive and his administrative assistants from the date upon which the executive commenced his employment with the company until they had an opportunity to interview both administrative assistants regarding the alleged complaint. Simultaneously, the internal investigations team processed the last two months of email and Slack communications between the executive and the administrative assistant in question.

While preservation obligations were triggered in relation to the administrative assistant who joined the corporation most recently, the internal investigations team made the correct choice to cast a broader net in preserving data generated by all three parties until they could satisfy the scope of their initial review.

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

Upon determining that a preservation obligation has been triggered,[62] 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" notice.[63] The style, content, and distribution of the legal hold notice will vary widely depending upon the circumstances, from a formal legal hold notice to an email communication. Regardless of form, the language used should be plain and provide clear instructions to recipients. The legal hold notice should set out in detail the kinds of information that must be preserved so the affected custodians can segregate and preserve it. Legal holds should not typically require the suspension of all routine records management policies and procedures. The legal hold notice should also advise the custodians that relevant documents can exist in multiple locations (i.e., networks, workstations, laptops, home computers, phones, tablets, voicemail, paper, etc.).[64]

---

62. 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.

63. "Legal hold" refers to the process by which an organization seeks to satisfy an obligation to preserve, initially by issuing a communication designed to suspend the normal disposition of information pursuant to a policy of through automated functions of certain systems. The term "legal hold notice" is used when referring to the actual communication. The term "legal hold" is used rather than "litigation hold" (or other similar terms) to recognize that a legal hold may apply in nonlitigation circumstances (e.g. pre-litigation, government investigation, or tax audit). See The Sedona Conference, "Commentary on Legal Holds, Second Edition: The Trigger & The Process" (2019) 20 Sedona Conf J 341 ["Commentary on Legal Holds"], online: The Sedona Conference <https://thesedonaconference.org/publication/Commentary_on_Legal_Holds>.

64. See the 'Key Factors to be Considered' when determining the scope of a particular hold, which include (i) the issues in dispute; (ii) accessibility; (iii)

The legal hold notice only needs to be sent to "affected" persons, i.e., those reasonably likely to maintain documents relevant to the litigation.[65] Custodian interviews often will help to identify which people actually hold relevant documents. The legal hold notice should 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 be held with the IT staff to ensure everyone understands what information must be preserved by the legal hold. The legal hold notice 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 notice should mention the volatility of ESI and make it clear that particular care must be taken not to alter, delete, or destroy it.[66] Once a legal hold is issued, this step is not over. It is advisable to resend the legal hold notice to the custodians at least every six months, and to ensure it is sent to any new employees to whom it may apply. There is case law in the U.S. that requires legal holds to be resent on a regular basis.

The legal hold should be personalized to the unique setup of the organization wherever possible in order to obtain maximum adherence from the custodians receiving the legal hold notice. For instance, if an organization maintains all project related

---

probative value; and (iv) relative burdens (costs) as defined in "Commentary on Legal Holds," *supra* note 63 at pp 391–95.

65. See *ibid* at pp 366–69.

66. 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>.

documents subject to the legal hold on a shared FTP[67] site, then the specifics of the FTP site should be included as a document category to the legal hold.

A legal hold notice should designate an individual within the organization (e.g., in-house legal counsel or alternatively a representative from upper management) to be the point person in the event that the recipients of the legal hold notice have any follow-up questions or concerns. It is always a best practice to have the recipients acknowledge receipt of the legal hold notice.

Custodians should be advised when a legal hold is lifted. When legal 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.* An organization 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 email and its website. As part of its contract for services, the organization requires the outsourcer to make weekly backups of the website and to keep the backup for six months, after which it would keep the last copy of the month. The organization issues a legal hold notice to the outsourcer asking it to suspend the deletion of the backup data until it can determine which backups would contain the version of the website corresponding to the time period mentioned in the claim.

67. FTP: File Transfer Protocol. See "Sedona Conference Glossary," *supra* note 1 at 311.

> *Illustration ii.* A former employee is suspected of having stolen client contact information and copies of design diagrams when she resigned to start a competing organization. The relevant systems can generate electronic reports that can be sent by email to a recipient. A legal hold notice should be sent to the organization's IT department asking that it preserve the log of the former employee's activities as well as any emails sent, received, or deleted from the former employee's account. The legal hold should also instruct the organization's IT department to refrain from reformatting or "wiping" the former employee's workstation and reassigning it to another member of the organization.
>
> The best evidence for the case, however, may be with the former employee. See discussion below on Anton Piller orders in Comment 3.i (Preservation Orders).

Comment 3.f. Preservation in the Province of Québec

In the civil law jurisdiction of Québec, the parties' obligations in the context of litigation differ from those 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.

Prior to the latest Québec *Code of Civil Procedure* coming into force in January 2016, there was no specific obligation to preserve electronic documents in advance of litigation. However, the Superior Court had 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.*[68]

In 2016, the duty of preservation was formally added as one of the "guiding principles of procedure" in the first paragraph of section 20 of the new *Code of Civil Procedure*:

> The parties are duty-bound to cooperate and, in particular, to keep one another informed at all times of the facts and particulars conducive to a fair debate and make sure that relevant evidence is preserved.

Comment 3.g. Privacy Obligations

Consideration should be given to any applicable statutory requirements or regulatory guidelines relating to the preservation, processing, or collection of personally identifiable information (PII).[69] Privacy law in Canada is a particularly fluid area of law, and there are currently a number of proposals to reform Canadian and provincial privacy legislation. Counsel should therefore always consult applicable legislation before applying these guidelines.

In Canada, the governing federal law relating to privacy in the private sector is the *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA governs the collection, use and disclosure of personal information in the course of commercial activities.[70]

---

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

69. The Sedona Conference, "The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines" (2020) 21 Sedona Conf J 577 ["Sedona Canada Commentary on Privacy and Information Security"].

70. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5., s 3 [*PIPEDA*].

Canadian private sector privacy legislation generally requires notice to and consent of the individual in order for an organization to use or disclose the individual's PII. There are exceptions to this requirement. In particular, notice and/or consent is not required to disclose an individual's PII where the disclosure is made in order to comply with rules of court relating to the production of records or a court or tribunal order.[71]

With respect to privacy concerns as they apply to document preservation, parties should generally ensure that documents are not being unnecessarily retained. This reduces the risk that an individual's personal information is compromised or unnecessarily viewed or disclosed. Many privacy laws also provide the individual a right to access and/or correct personal information collected or held by an organization. Parties should take care in reconciling this obligation with the obligation to preserve documents. For example, it may be that where an initially preserved document is corrected by an individual, both versions should be preserved.

Attention should be paid to the patchwork of national and subnational privacy laws that may apply to the personal information being preserved, including those in Canada, the United States, and the European Union.

For example, in Canada, PIPEDA applies to most commercial activity, but it applies to the employment context only where the employee is employed by a federal work or undertaking. Substantively similar legislation applies to employees in some provinces (British Columbia, Alberta, and Québec). Provinces also have specific privacy legislation that applies to the health-care sector.

In the United States, privacy obligations vary by state and sector.

---

71. *Ibid*.

In the European Union, the governing privacy law is the General Data Protection Regulation (GDPR).[72] While PIPEDA and the GDPR are essentially similar in spirit, there are nuances that need to be considered throughout the preservation, processing, and collection stages.[73] It is important that the correct regulations are followed when contemplating the appropriate preservation, processing, and collection methods. This can become particularly challenging for international corporations that operate in numerous jurisdictions.

> *Illustration i.* A Canadian business has received a statement of claim and is in the process of preparing a litigation hold for the preservation of data across its organization. While based physical in Canada, it has an e-commerce site that offers goods and services to individuals located within the European Union. Due to the interfacing of data with individuals within the European Union, the business will have to consider compliance with the GDPR.

Privacy obligations are discussed further under Principle 9.

---

72. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC [2016] OJ, L119/1 [GDPR], online <EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu)>.

73. According to *The Sedona Conference Commentary on Legal Holds*, "these (GDPR) laws and regulations may prohibit or restrict an organization from "processing" such data, including retaining it in situ outside of a routine schedule, or copying, moving or otherwise targeting it. . . ." See "Commentary on Legal Holds," *supra* note 63.

Comment 3.h. 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.[74] 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 data or other nonreadily accessible sources and the effort required to preserve them is not disproportionate given the issues and interests at stake, they should be preserved.[75]

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

While making forensic copies of hard drives is necessary in some cases for the preservation phase, processing the contents of the hard drives should not be required unless the nature of the matter warrants the cost and burden.[76] Making forensic

---

74. 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*].

75. *Mansfield v Ottawa*, 2012 ONSC 5208 at para 43 (CanLII) [*Mansfield*].

76. *Janzen*, *supra* note 27 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

images of devices including laptops, phones, and tablets is often not required and should be considered by counsel. 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 3.i. 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,[77] 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*.[78]

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

---

onerous expense militate against allowing such a search merely because it can be done."

77. 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.

78. *Celanese Canada Inc. v Murray Demolition Corp.*, 2006 SCC 36 (CanLII) [*Celanese Canada*].

the plaintiffs for Anton Piller relief in *CIBC World Markets Inc. v. Genuity Capital Markets*.[79] The defendants voluntarily undertook to preserve the electronic evidence and retained a forensic consultant to execute the preservation. The 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.[80] An Anton Piller order obtained ex parte was set aside where the plaintiff did not establish a real possibility that evidence may be destroyed.[81]

In *Portus Alternative Asset Management Inc. (Re)*,[82] 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 it specifically ordered the debtors not to alter, erase,

79. *CIBC World Markets Inc. v Genuity Capital Markets*, 2005 CanLII 3944.

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

81. In the *Velsoft* decision, *supra* note 41, 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.

82. Portus Alternative Asset Management Inc. (Re), 2005 28 OSC Bull 2670.

or destroy any records without the receiver's consent. The debtors were ordered to assist the receiver in gaining immediate access 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 email correspondence.

Lawyers must pay special attention to social media accounts as relevant sources of information and consider if preservation orders should be put in place as early as possible to avoid spoliation. In *Sparks v. Dube,*[83] the Court acknowledged that a preservation order may be granted to preserve the data from social media sites given that the removal of data from such sites does not create a discernable trail of evidence. In certain circumstances, seeking such an order may be necessary and advisable.

Comment 3.j. 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 or at significant costs to the organization. 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 that could paralyze

83. *Sparks v Dube,* 2011 NBBR 40.

the party's ability to conduct ongoing business. A party's preservation obligation should therefore not require freezing of all ESI, but rather only the preservation of the appropriate subset of ESI that is relevant to the issues in the action.[84] Proportionality should also be considered when preserving data.

Comment 3.k. 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 these media is to have a backup of active computer files in case there is a system failure or a disaster such 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

---

84. *Doust*, *supra* note 56 at para 27:

"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 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; *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.); *Janzen*, *supra* note 27; *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."

purchase new backup media or additional storage space until the preservation obligation has ended.

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 has the potential to cause substantially higher costs for evidence preservation and production in connection with litigation.[85] Organizations seeking to preserve data for business purposes or litigation should, if possible, consider employing means other than traditional disaster recovery backup media.

If a party maintains archival data, whether stored in the cloud or other offline media[86] 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

---

85. See *Farris v Staubach Ontario Inc.*, 2006 CanLII 19456 at para 19 (ON SC):

"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."

86. 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, USB devices, etc.

data on the party's systems.[87] These steps may include notifying persons responsible for managing archival data as appropriate.[88]

> *Illustration i.* Pursuant to an information technology management plan, once each day an organization routinely copies all electronic information on its systems and retains, for a period of five days, the resulting backup data 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 deletion of all existing backup data pending discovery in the case. Complying with the requested order would impose significant expense and burden on the organization, and no credible evidence established the likelihood that, absent the requested order, the producing party will not produce all relevant information during discovery.[89] The organization should be permitted to continue the routine deletion of backup data in light of the expense, burden, and potential complexity of restoration and search of the backup data.
>
> *Illustration ii.* An employee was dismissed for cause from an organization. Three months later, the former

87. *Mansfield*, *supra* note 75 at para 43.

88. Martin Felsky & Peg Duncan, "Making and Responding to Electronic Discovery Requests" (2005) LawPRO Magazine 11, online <https://www.practicepro.ca/wp-content/uploads/2017/06/2005-09-electronic-discovery-requests.pdf>.

89. *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."

> employee sues for wrongful dismissal. During the search for information relevant to the matter, counsel learns that the IT department routinely deletes user inbox emails older than 30 days in an effort to control the volume of email on its servers. The data from the last backup of the month is kept for a year before being deleted. As part of the preservation plan, the backup data that is three months and older is retrieved and safeguarded; counsel reasons that more recent backup data 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 emails advancing the employer's case and damaging the plaintiff's are found.

Finally, if it is unclear whether unique, relevant data is contained in backup data, the parties or the court may consider the use of sampling to better understand the data at issue. Sampling will help establish the degree to which potentially relevant information exists in the backups 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 data.

> *Illustration iii.* In the course of a search for relevant emails belonging to a custodian who left an organization's employ a number of years ago, the organization discovers that IT has kept email backup data for the past ten years. The backup data is identified by 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 at issue happened over a six-month period, and the party determines that if there were emails, they should most likely appear in

the middle of the period. Therefore, it would be reasonable for the organization to sample the backup data that was identified with the date in the middle of the range. If backup data of a particular server did not contain emails of the custodian, the backups for that particular server could be excluded from further searches.

Comment 3.l. 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 and are instead set up to reflect projects or matters that are worked on jointly. Such areas should be identified promptly and appropriate steps should be taken to preserve shared data that is potentially relevant.[90]

> *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: email, word-processing, and spreadsheet files on her workstation and on the engineering department's shared network drive, and 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

90. *Drywall Acoustic, supra* note 61 at paras 111–12.

should work with the IT department to include these in the litigation hold.

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.

Comment 4.a. The Purpose of Discovery Planning

The purpose of discovery planning[91] 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.[92] 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, preservation, collection, and processing of documents;[93] the

91. 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 publication 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.

92. *Drywall Acoustic*, *supra* note 61 at paras 81–84.

93. "Processing" means an automated computer workflow where original digital 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 may also entail identification of duplicates/de-duplication. Processing can also involve steps to deal with documents that require special treatment, such as encrypted or password-protected files. Parties should avoid making

review and production of documents;[94] the determination of how privileged documents are to be handled or other grounds to withhold evidence; costs; and the development of 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.

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 eDiscovery, reflecting recent judicial opinions and attitudes in Canada and other countries.[95]

---

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 emails and which time zone to use when standardizing DateTime values.

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

95. *Wilson v Servier Canada Inc.*, 2002 CanLII 3615 (ON SC) [*Wilson*] 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

"Common sense and proportionality" have been described as the driving factors of discovery planning.[96]

In Ontario, the *Rules of Civil Procedure* require the parties "to agree to a discovery plan in accordance with [Rule 29.1]."[97] The development of a meaningful 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 Québec, modifications to the *Code of Civil Procedure* introduced the notion of cooperation by requiring the parties to

---

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) [*Sycor*]. In dispute was the form of production in a case where just the cost of printing emails 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.

96. *Drywall Acoustic*, *supra* note 61 at para 84.

97. *Rules of Civil Procedure*, r 29.1.03(3) states that the plan shall include:

   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.

agree on a case protocol, in a new chapter regarding case management.[98]

In Alberta, rule 4.4 of the *Rules of Court* states that parties in a "standard case" may agree on a litigation plan. Rule 4.5 states that parties to a "complex case" must agree on a "complex case litigation plan."[99]

The Nova Scotia *Civil Procedure Rules* contemplate voluntary discovery plans agreed to by the parties. [100]

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 is a best practice whether or not such a plan is prescribed by the rules of court of the applicable jurisdiction.[101]

---

98. CQLR c C-25.01, s 148-160.

99. Factors to be considered when categorizing a case as a complex case in Alberta include: the amount of the claim, the number and nature of the claims, and the complexity of the action; the number of parties; the number of documents involved; the number and complexity of issues and how important they are; how long questioning is likely to take; whether expert reports will be required; and whether medical examinations and reports will be required. A complex case litigation plan may involve the setting and adjustment of dates, one or more case conferences, an agreement on a protocol for the organization and production of records, and the assignment of case management judge. *Alberta Rules of Court*, Rules 4.2, 4.4, 4.5, 4.6, 4.10(2), 4.14(1), 4.23(5), 4.33(2); *Ursa Ventures Ltd v Edmonton (City)*, 2016 ABCA 135 (CanLII); *Jacobs v McElhanney Land Surveys Ltd.*, 2019 ABCA 220 (CanLII).

100. *Nova Scotia Civil Procedure Rules,* r 16.05(1): "Parties may make an agreement for disclosure of relevant electronic information, and a term of the agreement prevails over an inconsistent provision of Rule 15 Disclosure of Documents, or this Rule 16." *See Annapolis Group Inc. v Halifax Regional Municipality*, 2019 NSSC 264 (CanLII).

101. For a sample discovery agreement and other model documents, see OBA, Model Precedents; "Commentary on Legal Holds," *supra* note 63.

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 email exchanges between counsel. A more complex case may require a series of in-person meetings and a more comprehensive plan.[102] 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."[103] The Courts have criticized counsel for failing to create a discovery plan and have in some cases sanctioned counsel conduct using cost rules.[104]

Parties may consider discussing how each party intends to use technology. Parties can avoid common misunderstandings if there is early agreement on the use of technology, including: search terms, selected metadata fields, de-duplication, email threading, assisted review, or active learning techniques. The

---

102. *Enbridge Pipelines Inc. v BP Canada Energy Company*, 2010 ONSC 3796 paras 3-4. The Court endorsed a discovery plan in a complex piece of litigation but emphasized that not every case would require this level of detail.

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

104. *Corbett v Corbett*, 2011 ONSC 7161 (CanLII) [*Corbett*]; *Petrasovic Estate v 1496348 Ontario Ltd.*, 2012 ONSC 4897 (CanLII) [*Petrasovic*]; *Siemens*, *supra* note 18; *Hryniak*, supra note 20; *1414614 Ontario Inc. v International Clothiers Inc.*, 2013 ONSC 4821 (CanLII) [*International Clothiers*].

parties should agree upon the production format, file naming, the treatment of families, and the fields to be exchanged.

Parties are encouraged to take advantage of all available technology to ensure the most efficient and effective possible outcome. See Principle 7 regarding the use of technology and Principle 8 regarding production specifications.

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 that 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 eDiscovery. Decisions made about eDiscovery from the earliest moment that litigation is contemplated will have serious impact on the conduct of the matter and the potential cost of discovery. 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 notice to the operations division, captures the hard drives and server email 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.
>
> 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 emails should have been preserved and reviewed; (c) the list of search terms is demonstrably too narrow according to its eDiscovery expert; and (d) backup media containing highly probative evidence should have been restored because active end-user email 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.

In some cases, a single meeting will not be sufficient for the development of an appropriate discovery plan. Accordingly, Principle 4 envisions an ongoing series of discussions.[105] Those ongoing discussions assist counsel when they encounter

---

105. See, e.g., *L'Abbé*, *supra* note 23 at para 19, 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) [*Kaymar*] at para 37 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."

unanticipated technical issues. In 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."[106] This obligation does not disappear because there is an order of the court regarding discovery.[107]

Comment 4.c. Preparation for the Planning Process

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 management protocols, and the IT manager or managers familiar with the organization's network, email, communication, and

106. *Kariouk*, *supr*a note 103 at para 42.

107. *International Clothiers*, *supra* note 104 at para 20.

backup systems. These individuals may also attend the discovery plan meeting(s) where appropriate. (See Comment 4.d. below). Parties may also benefit from the advice and expertise of in-house and external counsel resources, including eDiscovery specialists, clerks, and paralegals.

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 the following.

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.[108]

Each party should consider developing a data map to capture information about its own data sources and to track how each has been handled—whether preserved, whether collected, whether processed, file count and size, etc. In the initial stages of discovery planning, the parties may want to share their data maps (or summaries) so that they can speak intelligently about what must be collected, processed, and reviewed, what can be

---

108. *Canada (Commissioner of Competition) v Air Canada (TD)*, [2001] 1 FC 219 (CanLII) (FCTD) at para 27:

> "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."

treated as secondary (e.g., in a phased plan), what kinds of files may require special treatment, whether it will be necessary to engage forensic experts, and so on. Data maps, whether shared or not, help to focus and guide decision making so that challenges relating to data volumes, data complexity, cost, and timelines can be identified and addressed early in the process.

Whether or not data maps are developed and exchanged, parties should document all important steps in their handling of ESI through the use of collection logs, chain-of-custody forms, an inventory of data assets, and so on.

When good information governance practices are respected, there should be no need to turn to backup media for collection, unless there is evidence that there are records solely available on backup media. Refer to Principle 5 regarding accessibility.

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 consider whether to apply (potentially on an urgent basis) for court direction to ensure that relevant information is not destroyed.

Comment 4.c.iii. Collection and Processing

The parties should 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. Possible selection criteria used to determine 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.

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.

Depending on the nature of the dispute and factors such as whether some data sources might be hard to collect (as in cross-border litigation or where some information is stored in legacy systems), it can make sense to adopt a phased approach to eDiscovery. Just as some disputes proceed in a bifurcated fashion (liability first, then damages), some disputes lend themselves to phased or tiered discovery. Parties can agree to give priority to certain date ranges, certain custodians' files, and certain file types—for example, focusing on communications first, then turning to human resources and accounting files later. Parties might agree to a phased approach to all post-preservation stages of discovery (collection, processing, review/analysis, and production) or agree to only one or two.

Parties should be mindful that not all parties will have the same technical capabilities and resources. Given that courts have made it clear that discovery should be approached in a spirit of collaboration and cooperation, parties should make good-faith efforts to adopt approaches and specifications that are acceptable to all parties. For example, large entities that regularly exchange sophisticated litigation load files should not assume that this will be acceptable to all parties. The principles of proportionality and cooperation should inform parties' discussions on these matters.

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.[109]

Parties should discuss whether it is beneficial to consider a phased approach to the review. The use of technology and techniques like search terms, concept clustering, assisted review, and continuous active learning are particularly well suited to—and helpful in structuring—such an approach. Documents relating to different issues can be addressed in a desired sequence. Also, reviewers can work through batches of conceptually similar documents, thus reducing the mental effort of having to cross back and forth between different types of documents, as happens in traditional chronological linear review.

Even a party who does not have access to advanced tools and techniques may find that a phased approach can be beneficial. Subsets of documents—in whatever format—can be prioritized for review and production, perhaps on a rolling basis.

A phased approach may also increase the chances of an early resolution of the dispute.

Comment 4.c.v. Production

Parties should discuss the form in which productions will be exchanged—for example, which document types will not be

109. The Sedona Conference, "Best Practices Commentary on the Use of Search and Retrieval Methods in E-Discovery" (2013) 15 Sedona Conf J 217.

exchanged in original digital format and instead exchanged as images.[110] Parties would benefit from a detailed discussion even where source documents are in paper form, or where, as is commonly the case, source documents exist in both hard copy and digital format.[111] 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 rework.

Parties should discuss whether all original digital productions should include full text. Where images are being exchanged or the receiving party does not have access to a review platform, parties should consider whether images should be searchable PDFs.[112] All such format decisions should be discussed and agreed to.

Given that parties often have unequal resources, these questions of technology and file format should be discussed during discovery planning to facilitate a fair and efficient discovery process.

---

110. *See infra* Principle 8 regarding production formats. As noted there, parties should exchange documents in original digital format whenever possible.

111. *Logan v Harper*, 2003 CanLII 15592 (ON SC) [*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."

112. PDF: Portable Document Format. See "Sedona Conference Glossary," *supra* note 1 at 353.

Comment 4.c.vi. Timing

Counsel should discuss the schedule and timing for the processing, review, and production of ESI and should address the need for additional discussions throughout the matter and a resolution process for any issues that may arise.[113,114]

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 eDiscovery 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 on, then the meeting will have a greater likelihood of success. Multiparty actions and class actions, in particular, will benefit from such an approach. Even if no in-person meetings take place, the same principles apply: the parties should have clear

---

113. *Kaymar*, *supra* note 105 at paras 37–38, 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."

114. In *2038724 Ontario Ltd. v Quiznos Canada Restaurant Corp.*, 2012 ONSC 6549 (CanLII) [*Quiznos*] at paras 129-130, 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 original digital format; and, that while important, discovery plans can be modified.

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 eDiscovery 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 up front 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.[115]

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

An effective discovery planning process requires a meeting of the minds. The purpose is to facilitate proportionate

115. *International Clothiers*, *supra* note 104.

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,[116] names of custodians, systems from which information will be retrieved, and the eDiscovery process developed by the parties for use in the case. Discovery planning need 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 can focus on the substantive aspects of and strategies for their case.

Accordingly, parties are encouraged to describe the discovery 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, potentially saving the clients the time, money, and aggravation of having to redo 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 timeline for agreement on its terms.

---

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

If no response is received, the draft discovery plan may form the subject matter of a motion for court approval.[117]

Comment 4.f. Consequences of Failing to Cooperate

Courts have criticized counsel for failing to meet their discovery planning 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."[118]

While the courts have confirmed that 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 responsibility to cooperate and draft a plan.[119] 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.[120]

The parties continue to have an ongoing obligation to confer and make adjustments and disclosures where necessary.[121] Adverse cost consequences are a serious risk in discovery motions for parties who fail to act reasonably or fail to meet their obligations.[122] In Nova Scotia, the failure to come to an agreement on electronic disclosure results in the default provisions of Civil

---

117. Courts have exercised their ability to impose discovery plans. *Ravenda v 1372708 Ontario Inc.*, 2010 ONSC 4559 (CanLII); *TELUS Communications Company v Sharp*, 2010 ONSC 2878 (CanLII) [*TELUS*].

118. *Kariouk*, *supra* note 103 at para 3.

119. *Siemens*, *supra* note 18 at paras 79–84.

120. *Ibid*.

121. *International Clothiers*, *supra* note 104; *Siemens*, *supra* note 18.

122. *Corbett*, *supra* note 104; *Petrasovic*, *supra* note 104; *Siemens*, *supra* note 18.

Procedure Rule 16, which include an obligation to perform all reasonable searches, including keyword searches, to find relevant electronic information.[123]

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. Traditionally this includes emails and electronic files (such as Word, PowerPoint, and Excel documents) that can be accessed in the normal course of business. In addition to the traditional sources, there are many other sources of data that present unique challenges in terms of preservation, collection, processing, review, and production. The sources include, but are not limited to, social media platforms, websites, chats, and collaboration tools. 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 media, 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

123. *Velsoft*, *supra* note 41.

because they are more difficult to deal with than other data forms. This is not always the case.

Adequate information governance and records management policies help facilitate discovery by ensuring organizations know where their data is, what their data is, and how to access it. Additionally, well-implemented information governance and records management policies ensure organizations are properly conducting legally defensible data disposition, which ensures that data is disposed of in a timely manner when it is no longer required (either by law, or by business use). This increased management of data helps ensure necessary discovery records are "reasonably accessible" and irrelevant records are disposed of in accordance with the defensible disposition plan.

Backup data, whether in the cloud or on physical media, presents a unique challenge, as it is typically created for disaster recovery, not records management or litigation purposes, and is often not reasonably accessible. Backup data is always duplicative of the original data set and should only be accessed in rare circumstances when the requisite data is not available through standard data collection. [124,125]

---

124. *Ontario Public Service Employees Union (Pacheco) v Ontario (Solicitor General),* 2019 CanLII 118416 (ON GSB). The Court determined that the cost and the burden of delay are disproportionate to the probative value of the information that is likely to be discovered from a forensic study of the employer's ESI. In other words, the benefits likely to be derived from the employer's ESI are outweighed by the cost and delay that would be incurred as a result of a forensic investigation.

125. In *Verge Insurance Brokers v Richard Sherk et al*, 2016 ONSC 4007 [*Verge*], the Ontario Superior Court invoked the principle of proportionality to order the plaintiff in a conspiracy matter to provide documentary evidence of 66 backup tapes containing voluminous records of email communication. The defendant, a former employee of the plaintiff insurance broker, brought a motion for the production of these backup tapes. The plaintiffs sought to fend off this order by citing the onerousness and expense of reviewing and

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 media, 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*,[126] the Court considered the plaintiff's request that additional email contained in backup tapes be produced by the defendant bank for a period of almost three years. The defendant argued this would cost between $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 emails authored by [the bank's] employees. This is way too speculative." In the end, the Court ordered that the emails from only four employees be retrieved for a period of just over one month.

---

producing these backed-up records. To this end, they advanced affidavit evidence that the cost of complying with such an order could reach $300,000. Justice Turnbull ultimately held that while the cost of this order was exceptional, it was not disproportionate in light of the correspondingly sizeable breadth of litigation and damage amount claimed by the plaintiffs.

126. *Murphy et al v Bank of Nova Scotia et al*, 2013 NBQB 316 (CanLII).

In *Hudson v. ATC Aviation Technical Consultants*,[127] 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 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 refrain from ordering production of relevant documents. For example, in *Park v. Mullin*,[128] 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

127. *Hudson*, *supra* note 41.

128. *Park v Mullin*, 2005 BCSC 1813 (CanLII).

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.[129]

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 costs involved.[130] Information that is otherwise relevant may be excluded on the grounds that recovery of that information involves an inordinate amount of time or resources that are not commensurate with the potential evidentiary value.[131]

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.

---

129. Master Short's decision in *Siemens*, *supra* note 18 at paras 136-138 and 156, where he stated that Sapient's email retention policy that deletes emails 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.

130. *Descartes v Trademerit*, 2012 ONSC 5283 (CanLII); *GasTOPS Ltd. v Forsyth*, 2009 CanLII 66153 (ON SC).

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

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 an abusive email from his supervisor as part of an ongoing pattern of harassment. The employee claims that the email would have been sent 18 months ago. There is no backup data 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 email folders, including the deleted items folder, but the email 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 email, the Court accepts the defendant's argument that the probability of finding traces of an email 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 multimillion-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.

It is under extraordinary circumstances, which would be established on a case-by-case basis by a court without strict precedent, that the search and production from backup systems would be ordered.

Comment 5.b. Social Media, Smart Phone Data, and other Nontraditional Record Types

Increasingly, parties will be called upon to collect, review, and produce data that is not found within traditional sources of evidence like corporate email or a company network share. Evidence in today's litigation can exist in virtually any electronic space, including on smart phones, social media platforms, websites, fitness trackers, security monitoring systems, the internet of things, the computer systems of automobiles, etc. The collection, review, and production of these types of information present a variety of issues and challenges.

For example, identifying the content of a website over time may require specific captures of the website with some sort of time stamp to validate when the version of the website existed. The website capture will inevitably not have all the functionality of the live website, which may present a problem depending

on the issues in the case. Publicly available website archiving sites such as Wayback Machine might offer point-in-time captures of websites, but such captures are not always the full website, and for many websites the archive is limited.

Social media accounts often consist of many components, including posts and reactions to posts both in the form of text or emojis. Posts themselves could be text, video, or photos. Some social media platforms may be configured to only allow downloads of certain aspects of an account's content, such as a post, and then only with permission from the account owner, while leaving things like replies or reactions behind. Those reactions could be just as relevant to the matter as the original post. It also might be difficult to collect direct messaging from these applications. For example, capturing a YouTube account could involve downloading hundreds of gigabytes of videos and any posts respecting these videos. The question then arises as to how to cost-effectively store and review this data and even how to connect the posts to the videos during the review process or while presenting the evidence.

There are as many different sources of potential evidence as there are electronic devices, social media platforms, and internet sites. Parties need to understand where the evidence in their matter might exist, including embracing the notion that some evidence might be difficult to locate and collect, as well as the specific requirements for collecting this evidence as completely and defensibly as possible without unnecessarily increasing costs. Proportionality is key in this endeavour. If possible, it is prudent to discuss these issues with the opposing party and try to formulate a collection and production plan as part of the discovery planning process. Parties should consider whether a third-party vendor expert in collecting such nontraditional forms of data is required.

For further guidance on these issues, see The Sedona Canada Commentary on Discovery of Social Media.[132]

Comment 5.c. 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. As data sources become more complex, including third-party cloud-based repositories and collaborative spaces, the need for discovery support may expand beyond an organization's four walls. 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.

Cloud-based repositories and hosted solutions raise additional questions and create unique challenges for discovery, particularly when data is hosted across jurisdictions. These challenges include evaluating relevant privacy laws and third-party vendors' information governance and records management policies, including data disposition practices, and ensuring these align with the organization's own policies and guidelines, or that appropriate contractual agreements are in place to protect the organization's data.

---

132. The Sedona Conference, "The Sedona Canada Commentary on Discovery of Social Media" (2021) 23 Sedona Conf J 79 (forthcoming 2022), online: The Sedona Conference <https://thesedonaconference.org/publication/Sedona_Canada_Commentary_on_Discovery_of_Social_Media>.

Comment 5.d. Information Governance Policy

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 a 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;
- guidelines for the routine retention and destruction of ESI and paper documents, and for necessary modifications to those guidelines in the event of litigation;
- processes for the implementation of legal holds, including measures to validate compliance;
- 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, smart phones, text messaging, and other nontraditional data and data sources 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 standard category of business records listed in

an Information Governance Policy. Thus, while an Information Governance Policy should be consulted at the identification and preservation stages of eDiscovery, 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 to the court a more accurate picture of the cost and burden 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 *Commentary on Information Governance.*[133]

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

133. The Sedona Conference, "Commentary on Information Governance, Second Edition" (2019) 20 Sedona Conf. J 95, online: The Sedona Conference <https://thesedonaconference.org/publication/Commentary_on_Information_Governance>.

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.

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.[134]

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

In *Holland v. Marshall*,[135] the plaintiff's hospital records had been destroyed. At the time the records were destroyed, however, the hospital had a policy in place to destroy records for adult patients after the lapse of 11 years. The Court found that before the plaintiff's records were destroyed, litigation was not threatened nor reasonably anticipated by the hospital or any of the other defendants.

---

134. *Ireland*, *supra* note 27; *Doust*, *supra* note 56, 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.

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

In *Patzer v. Hastings Entertainment Inc.*,[136] 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.[137]

Information from social media that bases communication on timed data (which is deleted after a set period of time) can be relevant in certain cases. This content itself has been referred to as "disappearing content," or "ephemeral content." Information from these communication mediums can be valuable in court proceedings, and as such, has been requested. In an application for production of documents in *Araya v. Nevsun Resources Ltd*,[138]

---

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

137. *Strata Plan LMS 3259 v Sze Hang Holding Inc,* 2016 BCSC 32. The defendant invoked the concept of spoliation in order to invite the court to infer that the evidence (proxies used in shareholder votes) destroyed by the plaintiff would have undermined their legal position on the litigable issues. The court rejected this argument on the grounds that the failure to preserve the evidence was an intentional act done in bad faith to suppress the truth, a requirement of spoliation, could not be made out against the plaintiff. The non-preservation of the documents was consistent with its proxy retention policy of keeping ballots for only 90 days, and thus the plaintiff committed no wrong vis-à-vis evidentiary requirements and the provision of documents.

138. *Araya*, *supra* note 42.

personal communications were requested from platforms including Instagram and Snapchat, which use ephemeral content as a central method of communication. The production of these documents, however, is challenging. Discoverable documents are limited to those that are within a party's "possession, power and control." The question of whether parties must disclose ephemeral content depends on whether such communications are within a party's possession, power, and control. To answer this question, it is necessary to consult the policies of companies that use ephemeral content, such as Instagram, Snapchat, and Facebook.

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

Comment 7.a. Leveraging Technology Improves Efficiency and Reduces Time and Cost

Most individuals and organizations store vast amounts of digital information in many different forms and in multiple locations. Despite the volume, much of the information is likely to be irrelevant to any individual matter. Regardless of whether the litigation involves millions of records or just a few emails, finding the relevant information within this immense information store is akin to finding the proverbial needle in the haystack.

To best manage this volume of information, parties to litigation should discuss and agree on the implementation of appropriately targeted selection criteria to limit the preservation and collection of unnecessary data. However, information storage systems are generally not designed to efficiently find targeted information for eDiscovery purposes. Searching within many of these stores to find relevant records is often impractical or prohibitively expensive. To remedy this situation, consideration should be given to employing a variety of eDiscovery

methodologies and technologies. By targeting the identification, preservation, and collection of information, the result will be a much smaller dataset containing a higher percentage of relevant information that is ready for analysis, culling, and review.

When faced with multiple sources of data, the search and collection process should identify the most likely sources of relevant data in a manner that also optimizes time and cost effectiveness. Targeted selection criteria can be developed, tested through sampling, and then used to extract high-value data from the large collections of information.

Although the benefits of using electronic tools and processes for data sampling, searching, and review are obvious, especially when large volumes of electronic information are involved, these tools must be incorporated into a workflow process that ensures that they are used effectively and consistently so that the result is reliable and legally defensible. Put another way, it is imperative to develop and implement a defensible process. Smaller-volume collections may also benefit from the application of technology. Provided that the process is efficient and proportionate, there can be a significant return on investment for the use of technology instead of an exhaustive manual review.

Discovery tools are now mature technology that can make virtually every phase of eDiscovery more accurate (in terms of the quality of the results), more defensible (in terms of the processes involved), more efficient (in terms of resources), speedier, and even more cost effective than in the past.

Parties that deploy appropriate technology at the right stages of the discovery life cycle, and as part of well-planned and well-managed processes, will 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 relevant

documents than existed in the initial population (higher "recall"), while also handing over fewer nonresponsive documents than were traditionally included in productions (higher "precision").[139] These tools also offer the significant benefit of bringing the most important documents to the fore much earlier. The following sections discuss the most important uses of technology to achieve greater accuracy, efficiency, and savings.

Comment 7.b. Appropriate Technology as Part of a Defensible Process

The reliability and defensibility of the entire eDiscovery process is dependent on both the intelligent application of the appropriate tools and the process that is designed and put into place. Technology, workflows, and expertise must be applied together to develop and implement a defensible process. Legal advisors that rely on any technology to assist with the determination of relevance, privilege, or confidentiality should ensure that the tool is able to do what is claimed. This will require that the party using it has, at minimum, a basic level of understanding of how the tool operates and what it can do reliably. This may require that the technology and workflow are submitted to a validation or auditing process to ensure their efficacy. Parties may need to consult an expert to assist with understanding and managing the use of technology.

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 exact duplicate documents; (3) the search parameters to be used (e.g., date and other filtering processes,

---

139. For a full discussion of "recall" and "precision," see Comment 7.d, *infra*. For a comprehensive glossary of technology-related terms see Maura R. Grossman and Gordon V. Cormack, "The Grossman-Cormack Glossary of Technology-Assisted Review" (2013) 7 Fed Cts L Rev 1, online <https://www.fclr.org/fclr/articles/html/2010/grossman.pdf>.

search terms, conceptual search), and the use and application of technology-assisted review tools; and (4) the method for validating the results. Absent such an agreement, parties should document the process and methodology used, including decisions to include or exclude certain types or sources of documents, in order to defend the process in the event that the approach taken is challenged.

Comment 7.c. Party Self-Collection

Some parties want to conduct the collection of data themselves rather than outsourcing the work, both to minimize costs and to exert control over the process for reasons such as protecting employee privacy or confidentiality in corporate data. In doing so, parties may use the technical tools already available to them for their day-to-day work to assist with the discovery process.

For example, the features of Microsoft Office 365 offer preservation, searching, and collection across various applications such as Outlook, SharePoint, and OneDrive. Office 365 offers the ability to search Outlook email for keywords and time frames, and to de-duplicate the results upon export. Although such features do not render all data searchable, the risks of this might be acceptable in a particular case, especially given the cost savings likely to result from using these tools at the source of collection to cull data.

Microsoft Office products also offer legal holds on email accounts. This can be coupled with a Litigation Hold Notice to maximize the preservation of data.

Parties may also be able to do their own mass exports of data out of email platforms. Similarly, messaging applications like WhatsApp offer the same capabilities. In many cases, this type of collection will be sufficient. It is also cost-effective.

Comment 7.d. Techniques to Reduce Volume

Although technology and process should be used to target the identification, preservation, and collection of relevant data, generally the amount of effort should be proportional to the efficiencies to be gained. In other words, the identification, preservation, and collection process should not seek to be perfect in capturing only relevant information, although factors such as data security or privacy protections may require a high standard of accuracy at the collection stage. The process should be designed to weed out clearly irrelevant information, which is easier to identify, and leave the more refined culling to later stages in the eDiscovery process. This approach also ensures that relevant information that is difficult to identify up front is still preserved for later searching and, ultimately, production.

As a result, a significant portion of the ESI collected will still likely be irrelevant or only marginally relevant. It can be impractical or prohibitively expensive to manually review all the information collected. Parties should therefore consider, discuss, and agree on the use of appropriate processes and technologies to further cull the data so that the review process can be as efficient and cost-effective as possible.

As new technologies emerge, parties should assess them and (with the advice of experts, where appropriate) continue to embrace and apply them. That said, the most effective way to keep volumes of data as modest as possible is to maintain good, defensible information governance processes.[140]

Electronic tools and processes, such as the ability to run searches for words of similar meanings (i.e., concept search), and the ability to group and/or identify and tag collections of duplicates or near-duplicates in bulk can significantly increase

140. For a discussion of Information Governance, see *supra* Comment 3.b and Comment 5.d.

accuracy and efficiency and reduce the cost of the review process. 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 vetted methodology are adopted, and the results of the process are validated.

The best practice in Canada remains manual review assisted by technology for the document review phase. In some cases, the application of a variety of different types of technology may be the most effective approach. Parties should remain alert to new and evolving search and information retrieval methods as they emerge.

In assessing the use of technology, parties should consider the following:

a) In many settings involving ESI, the time and burden involved in a manual search process for the purpose of finding producible data may not be feasible, proportionate, or justified. Particularly in such cases, the use of automated search methods should be viewed as reasonable, defensible, and even necessary.

b) Success in using any automated search method or technology will be enhanced by a well-thought-out process with substantial human input and a clear plan to validate the results.

c) The choice of a specific search and retrieval method will depend on the specific context in which it is to be employed.

d) Good-faith attempts to collaborate on the use of particular search and information-retrieval methods, tools, and protocols, including keywords, concept search, technology-assisted

review, and other search parameters often result in cost savings and a more streamlined process.

e) Parties should expect that their choice of search tools and methodology will need to be justified, either formally or informally, after the process is complete.

Comment 7.d.i. Data Metrics Reports

Data metrics are a way to quantitatively describe a set of records. A data metrics report will typically include the overall volume of information, the number and volume of records for each type of data stored, records per custodian, document categories, and a breakdown of the records within certain date ranges. Effective data metrics reports will display this information in both tables and charts, so that an overall assessment of the nature of the data can quickly be obtained.

> *Illustration*. Prior to collection, the client requests a budget and information on the data being collected. To respond to that request, a data metrics report is generated with the help of the client's IT department. This report is then used to quickly identify the types of information and the location where relevant documents reside. Because photographs are not relevant to the case, the volume of digital photographs can be ascertained immediately, and the decision can be made to automatically identify and remove these records prior to processing or review. After the data is collected and processed, a more detailed report can be used to further cull irrelevant information before the data is subject to review. This information allows counsel to refine its initial budget prepared in answer to the client's questions.

Collecting information about the data 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 its technical advisors to understand and assess a document collection.

Comment 7.d.ii. Identifying Relationships Between Documents

Many documents are related in some way to other documents. For instance, data sources often include multiple copies of the exact same, or nearly the same, document, and individual emails are related to other emails in the same conversation chain. There are electronic tools available to identify such relationships between documents, so that the volume of records can be ascertained, and duplicative information can be set aside and eliminated from review.

A. De-Duplication

De-duplication or "de-duping" refers to the process of identifying exact duplicate[141] records. Once duplicates are identified, the copies can be set aside, so that only one copy of each record is actually reviewed. Records can be maintained (typically in a metadata field) of other custodians or sources that maintained

141. De-duplication should be limited to those documents that are exactly alike. Different discrete elements of documents can be compared, such as the textual content, or the actual bytes that make up the document, or a combination of specific elements or properties from a document such as the textual contents, author, creation date and time, size, and number of attachments. These elements can be combined to develop targeted de-duplication strategies appropriate for a particular matter. Most de-duplication processes will permit a producing party to maintain a record of the custodians or data sources from which duplicate copies were eliminated. It is a best practice to maintain such records.

duplicate copies. Depending on the case, de-duplication can save considerable amounts of time and money.

> *Illustration*. An organization with hundreds of employees will likely have hundreds of copies of a relevant organization policy that was emailed 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. The same situation can apply when all employees in a department save a copy of a contract to their individual hard drives. It is only necessary to review one copy of the contract.

While de-duplication can be performed individually within each custodian's data set ("vertical de-duplication"), most de-duplication tools are now able to keep track of the custodians who had duplicate copies (where it is important to know whether a particular document existed in the files of a particular custodian), allowing de-duplication to be performed across all files at once ("horizontal de-duplication").

Emails with attachments present a unique challenge when de-duplicating records. While stand-alone records (such as word-processing files) can be de-duplicated individually, emails with attachments should be treated as a single record for de-duplication purposes, to ensure that attachments are not inadvertently removed from their parent emails during the de-duplication process.

In some cases, the use of de-duplication tools may need to be tailored to suit the needs of a case, and parties may need to leverage specialized tools not commonly applied in the eDiscovery process. For example, in *LTS Infrastructure v. Rohl et al*,[142]

142. *LTS Infrastructure v Rohl et al*, 2019 NWTSC 10 [*LTS Infrastructure*].

a specialized geo-mapping tool and expertise were required to assist with the de-duplication of photographs that could not be de-duplicated using traditional eDiscovery technology.

Understanding the implications of de-duplication technologies and choices is an important part of discovery planning and the overall eDiscovery process.

B. Near Duplicates

The process of near-duplicate identification groups 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. Near-de-duplication can identify them so they can be reviewed together.

Using near-duplicate technology to group similar documents together and then highlighting the differences between the documents can help expedite the review process and ensure consistency in coding. This will save considerable time and cost and increase the quality and accuracy of the review.

> *Illustration.* In a contractual dispute, the review set contained twelve different versions of a contract. Each version was upwards of 100 pages, and the differences between them were minor, irrelevant to the dispute, and involved only a few pages spread throughout the contract. Near-duplicate technology was able to identify the twelve contracts in a single set of near-duplicate records. Using appropriate review tools, the first contract in the set was reviewed in its entirety, and the remaining eleven contracts were only checked for the differences between them, eliminating the need to review almost 1,100 pages of duplicate content.

Near-duplicate technology has many different configurations, allowing it to be used for several different purposes.

C. Email Threading

Email-threading technology identifies all individual emails that form an entire chain of an email conversation. The process also identifies the emails within the chain whose content is wholly contained in later emails. This allows review of the entire email conversation at one time and enables the review of only (a) the last or most inclusive email in a chain, and (b) any other emails that branch off or add something new that is not found in any other email or chain.

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.

D. Language Identification and Translation

Documents in a collection are sometimes written in different languages. Some emails and documents have different languages within the same body. Language-identification technology can identify all the different languages contained in the documents within the collection and record the percentage of documents in each language.

Once the primary or sole language of each document is identified, documents can be auto-translated or directed to reviewers who are fluent in each language, ensuring a more accurate analysis of the content.

In cases where a reviewer conversant in a particular language is not available, or only a rough understanding of the document's contents is required, language-translation technology can translate documents from one language to another within a matter of seconds or minutes, depending on the length

of the document. These machine translations are not usually accurate enough, on their own, to provide an exact translation or to discern nuance, but are usually good enough to understand the general content of a record.

Machine-translation services, combined with machine-learning processes, tend to yield much more accurate translations. This type of technology is typically used by service bureaus to translate large numbers of documents quickly, but it is also starting to be incorporated into eDiscovery review platforms to provide more accurate "on-the-fly" translations. It is recommended to always ensure that machine translation services are within the secure eDiscovery platform or provided by a trusted translation vendor to avoid the risks of sharing confidential or private data with online translation services.

Comment 7.d.iii. Keyword Search

Keyword search involves searching for documents containing one or more specific terms, such as product names and components in a product liability case.

There are pros and cons to using keyword searching as a means of locating documents that are relevant to a dispute. It is important to be aware of its challenges and limitations. Counsel should assess the best approach, which may be keyword searching or machine learning depending on the nature and volume of the records.

Pros of keyword search:

1. Keyword search can be a powerful tool when used in conjunction with other eDiscovery tools to organize, review, and perform quality control on a document set.
2. Exact or precise keyword search may help target specific information using a particular term or enclosing a phrase in quotes.

3. Boolean[143] and proximity operators in keyword search may increase accuracy.
4. Keyword searches can be done at any stage during a review. As more information is obtained about the matter, keywords can be refined.
5. Keyword analysis may be useful as part of quality control of a review effort or for sampling and validation processes.

Cons of keyword search:

1. Keyword search may exclude relevant information or include irrelevant information.
2. Ambiguous language, code words, and typos may result in missed relevant documents when using keyword search.
3. Syntax, punctuation, tokenization, case sensitivity, and non-English languages may pose challenges to accurate keyword search.
4. Specific languages such as Chinese, Japanese, Arabic, and Russian will require a different search engine than Roman-based languages like English.
5. Where there is more than one language in a data set, keywords may need to be translated into different languages. Literal translation is not always effective, since different phraseology may be used in different languages.

---

143. Boolean searches use keywords and logical operators such as "and," "or," and "not" to include or exclude terms from a search, and thus produce broader or narrower search results. See "Sedona Conference Glossary," *supra* note 1 at 276.

6. If a document has multiple fields that contain searchable text, such as the title, subject, and body, it is important to ensure that searches are applied to the proper field or across the multiple fields, if needed.

Illustration. It is important to understand how a particular search engine treats characters like hyphens. Not all search engines operate in the same way. Hyphens may be treated as a space, treated as a hyphen, or ignored in different systems. When the word "non-committal" is being searched, it may appear in the text index as "non committal," "non-committal," or "noncommittal." If hyphens are treated as a space by the search engine, then noncommittal would be missed in the search results. If the keyword is "committal" and the index contains "committal," "non committal," "non-committal," and "noncommittal," the search engine may miss "non-committal" and "noncommittal." It is therefore important to validate search terms and understand how the search engine operates to avoid errors.

Note that due to the casual nature of the language used in many emails, potentially relevant emails may not contain the exact 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 generally be validated through sampling both the responsive and nonresponsive populations.

Comment 7.d.iv. Machine-Learning Systems

Even after the volume of a party's ESI has been reduced by the use of various electronic filtering/culling processes, there

will still often be an overwhelming volume of ESI that must be reviewed for relevance, privilege, confidentiality, and personal information prior to production. Research in the information retrieval field has demonstrated that with large data collections, a review assisted by technology is more accurate than a manual, human review for the purpose of identifying relevant ESI.[144] It is generally accepted that a technology-assisted review will generally be less expensive than a manual review.

Machine-learning technology, also known as "technology-assisted review" (TAR) or "predictive coding," is a combination of technology and workflow that allows the computer to accurately identify the records in a data set that are most likely to be relevant or responsive.

The basic premise is that human reviewers, familiar with the issues in a case, "train" the machine-learning system to identify the relevant properties of a record by reviewing and coding a sample of records. As the reviewers code more records, the machine-learning system studies the properties of the records and develops a model (essentially a set of rules) that it uses to analyze unreviewed records to assess whether they should be coded as relevant. As the human review continues, the model is refined to the point where the machine-learning system can very accurately assess a record's relevancy.

Workflows and technology may vary in that the initial records selected for training the machine-learning system (the

144. Gordon V. Cormack and Maura R. Grossman, "Navigating Imprecision in Relevance Assessments on the Road to Total Recall: Roger and Me" (2017), Proceedings of the 40th Int'l ACM SIGIR Conference on Research and Development in Information Retrieval, online <https://dl.acm.org/doi/10.1145/3077136.3080812>; Maura R. Grossman and 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 1.

"seed set") may be selected through random sampling, or the computer may be fed human-identified relevant records ("judgmental sampling"). Some types of TAR simply group the records into three categories when the system has sufficiently learned what a relevant record is: likely relevant, likely not relevant, and indeterminate. Other types of TAR continue to analyze reviewer coding and update the model throughout the review, suggesting the next-most-likely relevant records for review until no more relevant records can be identified.

Machine-learning technology is well established in a number of review platforms, including several that are geared towards midsize litigation as well as those designed for large litigation. 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. Courts in many jurisdictions around the world, including the United States, United Kingdom, Ireland, and Australia, have accepted their use in eDiscovery,.[145]

It should be emphasized that the workflow and validation processes are critical when utilizing TAR to ensure defensibility, since the algorithms are based on probability and statistical analysis. Machine-learning technology on its own is not a substitute for the legal judgment of human reviewers. It is merely a tool that may be effectively applied in cases where keywords and other technologies are not likely to be as effective or are simply not feasible.

All the above tools can significantly increase not just the efficiency of a document review project but also its accuracy, and

145. *Rio Tinto PLC v Vale S.A.*, 306 F.R.D. 125 (2015) (collecting cases); see also The Sedona Conference, "TAR Case Law Primer" (2016) 18 Sedona Conf J 1.

at the same time reduce the overall cost. They 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 carefully vetted methodologies are adopted, and that the results of using any tools are appropriately validated.[146]

Comment 7.e. Sampling and Validating Results

All discovery processes should be subject to accepted methods of validation as appropriate under the circumstances.[147]

One approach commonly 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 an examination of the subset. Sampling can be carried out on a targeted basis ("purposive" or "judgmental" sampling) or systematically ("statistical" sampling). The most appropriate method will depend on the needs and circumstances of each case.

Sampling—whether judgmental 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 process. As with any tool used in eDiscovery, understanding how the tool works and why results are achieved is an important part of the process.

> *Illustration.* Where a party possesses a large volume of backup data, it may be appropriate to inspect the contents of a sample of the data to determine whether the inspection of the remaining data is necessary. In this case, determining what data to sample could be by

146. *Air Canada v West Jet*, 2006 CanLII 14966 (ON SC) [*Air Canada*].

147. *Verge*, *supra* note 125, as a caution with respect to the importance of validating a process.

> random selection, or by using common sense, informed by the client's understanding of where relevant ESI would be most likely to reside. If the latter approach is taken, this would be purposive or judgmental sampling.

The above illustration 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 the group-share contain evidence that is relevant. This high cost/low return ratio (or low "marginal utility" ratio) may weigh against the need to search that source any further,[148] 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*[149] for an application of cost shifting in an analogous situation.

> *Illustration.* During a review process, the legal team identifies a pattern of records that appear to be consistently irrelevant. Using keyword search, a large subset of the records is identified as potentially irrelevant. A statistical 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.

148. *McPeek v Ashcroft*, 212 F.R.D. 33, 37 (D.D.C. 2003).

149. *Consorcio Minero Horizonte S.A. et al v Klohn-Crippen Consultants Limited et al*, 2005 BCSC 500 (CanLII).

There are two statistical measurements that are typically used to measure the results of an information retrieval effort.

1. **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 search-and-review process finds 50 of them, the recall would be 0.5 or 50 percent. Recall measures how completely a process has captured the target set. High recall means that there are very few relevant documents that were missed (a low "false negative" rate); low recall indicates a higher proportion of false negatives.

- Higher recall generally supports the position that a party has met its production obligations when considered in the context of other appropriate quality assurance efforts.

2. **Precision**: The percentage of documents retrieved and identified as relevant that are in fact relevant.

- If 50 records are identified as relevant but five of them turn out to be nonrelevant, the precision is 0.9 or 90%.
- Precision measures how well a process has avoided including irrelevant records or "junk." High precision means there are very few documents in the result set that are not relevant (a low "false positive" rate); low precision indicates a higher proportion of false positives, in other words that the production set contains a significant amount of "junk."
- A higher precision helps avoid reviewing too many irrelevant records and therefore reduces cost.

Accordingly, the goal of any search-and-review effort is to achieve both high recall and high precision. Regardless of the technology used, or whether the documents are in hard-copy or electronic form, a reasonable method for validating the search-and-review process should be developed, including selection of an appropriate sample, analysis of that sample, and taking any remedial efforts that may be indicated as a result of the sampling process. The sampling or validation process that is warranted will vary by matter. A method suitable for one matter may not be applicable to a different matter. Consultation with an expert may be needed to design the most appropriate sampling or validation process in a particular matter.

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

Comment 8.a. Electronically Stored Information Should Be Produced in Electronic Form (Not Hard Copy)

When at all possible, the production of ESI should be made in searchable electronic form,[150] unless the recipient cannot effectively make use of a computer.[151] Examples of searchable

150. Discovery Task Force, *Guidelines for the Discovery of Electronic Documents* (2005) at Principle 11: "Production of voluminous documentation in a form that does not provide meaningful access should be avoided."; *Cholakis*, *supra* note 6 at para 30: "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."

151. 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: "[W]hile electronic or soft copy disclosure may now in the 21st Century be considered

electronic formats include original file formats (such as Microsoft Word, Microsoft Excel, and Microsoft Outlook files) and imaged representations of the original file formats (such as TIFF[152] or PDF) converted to a searchable form.

The practice of producing ESI in static form without accompanying metadata, such as by printing in hard copy, should be discouraged in most circumstances for several reasons:

- Depending on the nature of the electronic record, hard copy may not be an authentic substitute for the contents and properties of the original record.
- Hard copy does not 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.
- Hard-copy documents may require objective coding to provide basic identifying information for each record, i.e., document title, date, author, recipient, document type, etc. This increases the cost and time required to prepare the productions.
- Hard-copy records are harder to search and harder to logically organize using litigation support software tools. This means that a hard-copy production set is usually less usable than a set of

a usual form also, in the circumstances of this case, it is not accessible to the accused."

152. TIFF refers to "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" filename suffix.

documents produced in a searchable electronic format.[153]

- Reviewing a large collection of hard-copy records is more time consuming and expensive than reviewing the same collection of searchable electronic records,[154] since parties will not be able 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 multiparty actions, where savings can be significant.

---

153. *Wilson*, *supra* note 95 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 CanLII 7369 (OC GD).

154. *Sycor*, *supra* note 95; Where the cost of printing and photocopying email for production was estimated at $50,000, "At 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."

- Producing documents in electronic format is better for the environment.

Comment 8.b. Agreeing on a Form of 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, including the metadata fields it is seeking. Where scanned hard-copy records are being produced, the parties should also agree on which fields must be objectively coded. Given the fact that there are so many different litigation support programs available, each party may have different production requirements. While it is acceptable for the parties to produce documents in different formats (even within the same production), it is strongly recommended that parties develop a framework for resolving disputes over the form of production.[155]

For a number of reasons, ESI should wherever possible be produced in original digital format. First, the original digital version is the truest, most accurate version of the document; second, original digital files are easier, faster, and cheaper to transfer, upload, and search than any other format; third, conversion to other formats entails the loss of information; and fourth, original digital versions contain all of the application-level and user-created metadata, some of which may be crucial to understanding the context and meaning of the files. User-generated metadata is information about the document that is entered by a user at the file level such as, for example, the fields that can be populated in the "Properties" tab of a Microsoft Office

155. *Kaymar*, *supra* note 105: The Master observed that a well-crafted discovery plan that contains dispute resolution mechanisms can avoid motions practice, including on issues such as the form of production.

document. In addition, many kinds of electronic files contain information that can be lost if the file is simply converted to an image format. Examples of such information include that which is: (a) in spreadsheets, such as macros, formulas, conditional formatting rules, and hidden columns/rows/worksheets; (b) in presentations, such as speaker notes; (c) in word-processing documents, such as text-editing notations ("track changes"); and (d) in virtually all file types, such as comments, electronic sticky notes, and highlighting. Such information is as much a part of the document as the visible text and, in some investigations or litigation, can be highly relevant. Parties should therefore be prepared to produce files in their original digital format, or explain why they prefer not to or are unable to do so. Parties should also be aware that most modern processing tools can extract metadata that indicates whether an individual file contains certain kinds of normally hidden information, and these metadata fields (e.g., "contains hidden text") can be provided as part of the production.

Where parties prefer to produce or receive files converted from original digital 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 or TIFF format, however, does not preclude another party from asking that the production to it be made in its original digital format.[156]

---

156. *Quiznos*, *supra* note 114 at paras 128–31. The Court disagreed with the defendant's refusal to reproduce copies of Excel documents in Excel format. The documents had originally been produced in TIFF form 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.

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 on the redacted images and including the resulting text in the production. If the text of the document that has been extracted directly during processing is to be produced, the producing party should confirm that the redacted text is removed from the extracted version of the text, as well as from the image.

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 generally required 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 or searchability of produced information without the consent of the receiving party or an order of the court.

When compiling electronic documents for production, consideration should be given to processes that enable the efficient identification and retrieval of information required for discovery, witness preparation, and trial. In order to produce documents in a manner that meets discovery obligations, cooperation between the parties is required.[157] In *Bard v. Canadian Natural Resources*,[158] the Court noted that parties need to be able to manipulate electronic data, and the Court must therefore take a pragmatic approach as to what constitutes meaningful disclosure.

---

157. *City of Ottawa v Suncor Energy Inc.*, 2019 ONSC 1340, [*Suncor*] at paras 36–41.

158. *Bard v Canadian Natural Resources*, 2016 ABQB 267.

If the relevant documents contain foreign language, the parties should consider whether translation is required, the appropriate method of translation, and the allocation of the associated costs.

There is also an expectation that trials will increasingly be conducted electronically (which requires that documents be produced in an electronic form). In *Bank of Montreal v. Faibish*,[159] the Court rejected the proposition that the trial be conducted using both hard-copy 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."[160]

Comment 8.c. Agreeing on the Scope of Production

Taking into account Sedona Canada Principles 2 and 4 addressing proportionality, counsel for the parties must consider the nature of the case and determine the most likely sources of relevant information. Those sources might include computers and other electronic devices, including mobile devices, external media (such as hard drives, USB devices,[161] and disks), paper files, photographs, videos, voicemail, text messages, and all manner of social media.

An agreement among counsel with respect to the scope of production of information is important. Particularly in the case of ESI that is volatile or ephemeral, such as text messages, web pages, or social media accounts, early consideration should be

---

159. *Bank of Montreal v Faibish*, 2014 ONSC 2178 (CanLII).

160. Although this type of decision was rare at the time of the drafting and publication of earlier editions of *The Sedona Canada Principles Addressing Electronic Discovery*, it is anticipated that this type of decision and order will become increasingly common.

161. USB devices such as flash drives can be plugged into a Universal Serial Bus port on a computer as a means of transferring or extracting data. See "Sedona Conference Glossary," *supra* note 1 at 385.

given as to how that data is managed. In *Saskatoon Co-operative Association Limited v. UFCW, Local 1400,*[162] the Court took issue with the description of documents to be produced and held that the request for documents to be produced cannot be so broad that it may be considered a fishing expedition. The Court stated that consideration should be given to the documents requested for production such that efficiency of production can be achieved. Regarding social media, the Court stated consideration should be given to what kinds of social media may be relevant.

Comment 8.d. 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 sufficient 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."[163] 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.

These requirements date back to an era when parties produced only hard-copy documents. The document list was the only method of providing organization to a hard-copy

---

162. Saskatoon Co-operative Association Limited, v UFCW, Local 1400, 2019 CarswellSask 346.

163. 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 either an affidavit of documents or list of documents.

collection. This practice remains today, although as noted below, it is evolving.

Where parties exchange hard-copy productions or electronic productions of hard-copy records that have been digitized, the document lists are usually manually coded using information obtained from the content (i.e., face) 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 (for original digital, or other electronic productions), parties should consider using the metadata associated with the records to populate the standard fields identified above instead of manually coding information from the content of the record, even if the original digital files are converted to an image format prior to production. This practice is particularly applicable to the production of emails, where the metadata clearly indicates the Record Type, Author, Recipient(s), Record Date, and Record Title (subject). For non-email records, the metadata, file type or file extension can be used to denote the Record Type, the file name or path name could represent the Record Title, and the last modified time stamp could represent the Record Date. The suitability of using metadata instead of manually coded information should be based on whether the metadata is known to be reasonably accurate and whether using the metadata will result in the production of information sufficient to uniquely identify each record being produced.[164]

As noted above, the need to provide these "lists of documents" is evolving, given the nature of electronic documents and the ways in which they can be searched and sorted.

164. *Canadian Imperial Bank of Commerce v R.*, 2015 TCC 280 at paras 232–43.

Document lists often are part of an affidavit that must be sworn by the client 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 identification, collection, processing, and review of the documents exchanged in production.

Comment 8.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.[165] 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 *Tk'emlups te Secwepemc First Nation v. Canada*,[166] the Court ordered that a party has a positive obligation to assist the opposing party to

165. Coding: An automated or human process by which specific information is captured from documents; see "Sedona Conference Glossary," supra note 1 at 325.

166. *Tk'emlups te Secwepemc First Nation v Canada*, 2020 FC 399 (CanLII).

better manage and understand large document production, including whether the government was required to disclose the field names or rules used to populate the fields with readable content, and whether such disclosure would compromise solicitor-client privilege. Canada was ordered to disclose the field names it has used in the organization and management of its documents, to the extent known and the rules used to populate the fields.

- In *Seifert v. Finkle Electric Ltd.*,[167] it was argued that the affidavit of documents failed to individually list and identify each document. Each document was required to have a unique number so it could be separately identified. Numbering the pages within the listed collection of documents or file fails to provide a sufficient identifier of the individual documents contained within the collection.
- In *Cameco Corp v. Canada*, [168] the respondent argued the use of metadata to describe all documents was unsatisfactory and had resulted in a "maldescription" of documents. The Court held that as long as the appellant had provided a sufficient description of the documents using a numerical identifier for each document, its identification of the document was satisfactory, and metadata-based identifiers were allowed.

167. *Seifert v Finkle Electric Ltd.*, 2020 ONSC 394 (CanLII).

168. *Cameco Corp. v Canada*, 2014 TCC 45 (CanLII).

- In *LTS Infrastructure v. Rohl et al*,[169] the parties agreed that metadata would be used instead of objectively coded data for all records and also agreed that hard-copy documents would be scanned and produced electronically in searchable PDF format with objective coding.
- In *HRD Kitchen Services (Toronto) Ltd. v. Prime Food Equipment Services Ltd.*,[170] the Court ordered that counsel must devise a system of document production that satisfies the spirit and intent of the rule and that contributes to the efficient resolution of the litigation. Although the onus of complying with obligation of documentary production rests on the party responsible for producing the documents, there is an expectation of collaboration.
- In *Wilson v. Servier Canada*,[171] the Court granted the plaintiff's motion for an order directing the defendant to release the objective coding of the documents in its litigation support database in order to meaningfully satisfy its disclosure requirements, given the volume of documents.
- In *Logan v. Harper*,[172] the defendants had produced the documents along with a searchable index in electronic form. The index did not permit full-text searching of the documents, although the version of the application used by counsel

169. *LTS Infrastructure*, *supra* note 142.

170. *HRD Kitchen Services (Toronto) Ltd. v Prime Food Equipment Services Ltd.*, 2017 ONSC 559 (CanLII).

171. *Wilson*, *supra* note 95.

172. *Logan*, *supra* note 111.

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 license for the software for access to the full-text search feature.

- In *Jorgensen v. San Jose Mines et al*,[173] the defendants sought delivery of the electronic database used by the plaintiff to compile the list of documents. The Court ordered the plaintiff to provide a copy of the database to the defendants in electronic form and ordered the defendants to pay $4,000 to the plaintiff's firm as a reasonable proportion of the costs of preparing the database.
- In *Gamble v. MGI Securities Inc.*,[174] 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 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

173. *Jorgensen v San Jose Mines et al*, 2004 BCSC 1653 (CanLII).

174. *Gamble v MGI Securities Inc.*, 2011 ONSC 2705 [*Gamble*].

> resources of the two parties—the plaintiff being a former employee of the corporate employer. It is noteworthy 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 reviewing documents to be produced will normally be borne by the producing party.

Given the advances in technology and search functionality, parties often agree not to exchange objective coding fields to reduce unnecessary costs. In some cases, however, it may still be appropriate to do so.

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 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 is often 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.[175] Nevertheless, one court has 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 evidence that could serve that purpose.[176] In contrast, see *L'Abbé v. Allen-Vanguard Corp.*,[177] 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 asserting the privilege or certain other conditions are met.[178] Privilege

---

175. See *Elliot v Toronto (City)* (2001), 54 OR (3d) 472 (SC) at para 10; 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 CanLII 563 (BC SC); *National Bank Financial Ltd. v Daniel Potter et al*, 2005 NSSC 113 (CanLII); *National Bank Financial Ltd. v Daniel Potter*, 2004 NSSC 100 (CanLII); *Autosurvey Inc. v Prevost*, 2005 CanLII 36255 (ON SC), *O'Dea v O'Dea*, 2019 NLSC 206.

176. See *Metcalfe v Metcalfe*, 2001 MBCA 35 (CanLII) at para 28.

177. *L'Abbé, supra* note 23; *Minister of National Revenue v Thornton*, 2012 FC 1313 (CanLII); *McDermott v McDermott*, 2013 BCSC 534 (CanLII).

178. See *Canadian Imperial Bank of Commerce v The Queen*, 2015 TCC 280, where the Court denied CIBC's request to re-review certain records previously coded by a third-party provider as subject to litigation privilege to determine whether the records were also covered by solicitor-client privilege, after the litigation had concluded and the records were no longer subject to litigation privilege. The Court held that in this case, where there were already significant delays, it would be unfair to the opposing party to allow the further review.

may be lost through inadvertent disclosure based on considerations including: the manner of disclosure, the timing of disclosure, the timing of assertion of privilege, who has seen the documents, prejudice to either party, or the requirements of fairness, justice, and the search for truth.[179]

The issue of volume was addressed in *L'Abbé v. Allen-Vanguard Corp.*, where the Master held that court inspection of 6,000 inadvertently produced documents over which privilege was claimed was not a viable option. Instead, the Master placed on the parties the obligation of narrowing the dispute in relation to those documents. In so doing, the Master directed the parties to first try to reach agreement with respect to probative value and relevance of the documents, and then to attempt to come to agreement on categories of 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."[180]

179. The Federation of Law Societies of Canada's 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. online: <https://flsc.ca/wp-content/uploads/2014/10/ModelCodeENG2014.pdf>. This principle has been adopted by Law Societies in Canadian jurisdictions. See *Aviaco International Leasing Inc. v Boeing Canada Inc.*, 2000 CanLII 22777 (ON SC) at para 10-13.

180. *L'Abbé*, *supra* note 23 at para 98.

Comment 9.a.ii. Preventative Measures

With the massive number of electronic documents typically 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[181] 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. However, it is important to recognize that searching for words and phrases to identify privileged records will often cast a wide net, yielding both over- and under-inclusive results. Absent in-depth knowledge of the data, keyword lists cannot be drafted to identify all and only privileged content.

To overcome the limitations of keyword search and manual review, machine-learning tools such as concept clustering and technology-assisted review that build models can be used to assist with the identification and segregation of potentially privileged records. These types of analytics may combine unsupervised and supervised learning techniques to predict the likelihood that a document contains privileged subject matter.

In many cases, a combination of one or more of the methodologies described above will be useful. There is a growing body of evidence from the field of information retrieval that the use of technologically based search tools may be more efficient and

181. *Air Canada*, *supra* note 146 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 23.

more effective than manual review.[182] It is therefore recommended that consideration be given to this body of evidence in assessing whether reasonable steps were taken in a privilege review.

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 have included 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 direction from the Court or to stop the review and notify the privilege holder.[183]

---

182. See, e.g., Feng C. Zhao, Douglas W. Oard & Jason Baron, "Improving Search Effectiveness in 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 1; Peter Gronvall et al, "An Empirical Study of the Application of Machine Learning and Keyword Terms Methodologies to Privilege-Document Review in Legal Matters" (2018) IEEE International Conference on Big Data.

183. *National Bank Financial Ltd. v Daniel Potter*, 2004 NSSC 100 (CanLII); *Autosurvey Inc. v Prevost*, 2005 CanLII 36255 (ON SC); *Celanese Canada*, *supra* note 78; *Nielsen v Nielsen*, 2017 BCSC 269 (CanLII); *Tiger Calcium Services Inc. v Sazwan*, 2019 ABQB 500 (CanLII); *888 Fort Street Holdings Ltd. v Ross*, 2017 BCSC 579 (CanLII).

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.[184] One benefit of a court-appointed neutral expert is the probable elimination of privilege waiver concerns with respect to the review of information by the 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. 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.[185]

Comment 9.a.v. Protection of Privileged Information

Given the expense and time required for pre-production review 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"

184. *Catalyst Fund General Partner 1 Inc. v Hollinger Inc.*, 2005 CanLII 30317 (ON SC).

185. *Celanese Canada*, *supra* note 78; *Solicitor-Client Privilege of Things Seized (Re)*, 2019 BCSC 91 (CanLII).

agreements.[186] 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 that any dispute will be submitted to the court. It is preferable that any such agreement or order be obtained before any production of documents takes place. The agreement should clearly specify the process and steps to be taken in the event a party or its counsel determines that a privileged communication has been inadvertently disclosed.

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 forth principles to be considered in such determinations.[187] Also, a clawback agreement may not be enforceable against a party who is not a signatory to the agreement.[188]

Parties continue to find new and innovative ways to identify privileged documents more efficiently and effectively than through manual review alone. Courts have considered the use of technology tools, both in evaluating pre-production search methodologies and in determining whether privileged

---

186. *Air Canada*, *supra* note 146; *Suncor*, *supra* note 157; *Zubulake v UBS Warburg* LLC, 216 FRD 280, 290 (SDNY 2003) (WL).

187. *Nova Chemicals (Canada) Ltd. v Ceda-Reactor Ltd.*, 2014 ONSC 3995 (CanLII); *Township of Neshannock v Kirila Contractors, Inc.*, 181 A.3d 467.

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

documents were recklessly produced, or if reasonable good-faith efforts to exclude privileged documents were made.[189]

Comment 9.b. Confidential Information Issues

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 in the course of discovery. The availability of protective orders is the product of an attempt to balance the competing considerations 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)*,[190] 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[191] was rejected, and the appeal from this decision was dismissed by all but one judge

189. *The Commissioner of Competition v Live Nation Entertainment, Inc et al*, (2018) CACT 17 (CanLII) [*Live Nation*]; *L'Abbé*, *supra* note 23 at para 98.

190. *Sierra Club of Canada v Canada (Minister of Finance)*, 2002 SCC 41 (CanLII) [*Sierra Club*].

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

of the Federal Court of Appeal.[192] On further appeal to the Supreme 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.[193]

A Norwich Order is a remedy that compels third parties to disclose information that cannot otherwise be obtained and that

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

193. *Sierra Club*, *supra* note 190.

a claimant may need before commencing a lawsuit. This is a controversial and exceptional equitable remedy that compels a third party to disclose information that may be private or confidential in nature. Courts will avoid granting a Norwich Order unless a claimant can show why such disclosure is necessary and just under the circumstances. In *Carleton Condominium Corporation No. 282 v. Yahoo! Inc.*,[194] the Court considered the balance of the benefit to the applicant of disclosing the requested information against the prejudice to the alleged wrongdoer in releasing the information and ultimately found that disclosure was necessary to identify the original author of the emails at issue.

In addition to clawback agreements, parties may find other ways to protect privileged, confidential, or sensitive information while balancing fairness and the obligation of disclosure. For example, the Court in *Guest Tek Interactive Entertainment Ltd. v. Nomadix Inc*.[195] permitted certain commercially sensitive documents to be designated as "Counsel's Eyes Only," which were not to be disclosed to any officer, director, or employee of Guest Tek, but could be disclosed to Guest Tek's external experts and consultants retained for the purpose of the litigation.

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

194. *Carleton Condominium Corporation No. 282 v Yahoo! Inc.*, 2017 ONSC 4385 (CanLII).

195. *Guest Tek Interactive Entertainment Ltd. v Nomadix Inc.*, 2018 FC 818 (CanLII).

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. These electronic tools can perform functions such as:

- Auto-Redaction: typically an add-on to a review platform that identifies and searches for certain patterns and applies redactions to them. Such patterns can include sensitive data such as Social Insurance Numbers, credit card numbers, and personal information (addresses, phone numbers, etc.);
- Entity Extraction: the use of machine-learning techniques to identify personal, privileged, or sensitive information that may require redaction;
- Redaction of original digital records: redaction of a copy of the original digital document may be required if imaging the original document is infeasible; and
- Anonymization and Pseudonymization: Anonymization involves the deletion of all personal identifiers in a document, typically by applying redaction. With pseudonymization, the identifying information is removed in such a way that with additional information, the individual can be reidentified. Such tools may retain the links between multiple records pertaining to the same individual.

Regardless of the tools or methodology used to apply redactions, additional quality control steps are generally necessary to

ensure that the protection of personal, confidential, or privileged information has been properly achieved.

Comment 9.c. Privacy Issues

Canada and its provinces, to varying extents, have comprehensive privacy legislation[196] governing the collection, use, and disclosure of personal information,[197] 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.

While Canadian private sector privacy legislation typically requires consent of and notice to an individual before the individual's personal information is disclosed, disclosure required by the rules of court or a court or tribunal order is typically exempt. Further, the prevailing view is that Canadian private

196. 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-22.01; *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*, 2015, SNL 2015, c A-1.2. Legislation governing the private sector includes the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5. [*PIPEDA*].; *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.

197. Personal or private information is generally defined as information about an identified or identifiable individual.

sector privacy legislation does not apply to personal information collected for purposes of litigation.[198]

This does not mean, however, that parties should ignore privacy concerns. Parties and their counsel should ensure that proper safeguards are incorporated into the review and disclosure of ESI containing personal information. Failure to apply appropriate safeguards could give rise to privacy complaints if personal information is collected, reviewed, or disclosed where not strictly required by court rules or orders. Further, international privacy laws may apply to ESI relevant to Canadian proceedings and may not have the same exemptions for litigation purposes.

Parties should ensure their compliance with applicable privacy law regimes in Canada and internationally.

Parties and their counsel should avoid unnecessarily seeking or disclosing irrelevant personal information, particularly the personal information of third parties not involved in the litigation.

Privacy concerns are heightened when the personal information involved is particularly sensitive. The sensitivity of personal information lies on a spectrum and is context-specific, with certain types of information typically seen as highly sensitive (e.g., certain financial information, Social Insurance Number, sexual history) and other types of information as less sensitive. While there is a general obligation to avoid disclosure of irrelevant PII in litigation, the reasonable steps that must be taken to ensure that irrelevant PII is not disclosed may vary depending on the circumstances, taking into account

198. *Ferenczy v MCI Medical Clinics*, 2004 CanLII 12555 (ON SC); *State Farm Mutual Automobile Insurance v Privacy Commissioner of Canada*, 2010 FC 736 at paras 98–100, 106–07 (CanLII); *Hatfield v Intact Insurance*, 2014 NSSC 232 at para 27 (CanLII). In contrast, see *PIPEDA Case Summary No 2011-003, Re*, (March 25, 2011) 2011 CarswellNat 6886.

proportionality considerations. As a general matter, more stringent precautions should be taken to protect highly sensitive PII, while it may be acceptable in some cases to take less stringent precautions to protect PII that is not particularly sensitive. In considering the options for protecting PII through redaction or other measures, counsel should be aware of and consider the latest technological options, including auto-redact features in litigation support software tools that will look for and redact text or numbers that appears to be PII (e.g., Social Insurance Numbers).

As discussed in Comment 9.b, parties can obtain a court order or incorporate terms into a discovery plan for the redaction of irrelevant personal information.

The courts have not been sympathetic to objections to producing relevant information based on privacy concerns.[199] Courts do, however, consider privacy issues in assessing whether discovery requests are overly broad or whether non-relevant private information can be protected.[200]

It is important to note that the deemed undertaking rule[201] and the implied undertaking rule are rules in the discovery process only. They do not provide complete privacy protection either within or outside of the litigation process. For example, in Ontario, the deemed undertaking rule applies only to evidence

---

199. See *M(A) v Ryan*, [1997] 1 S.C.R. 157 (CanLII), where the Court determined that the disclosure of private documents may be necessary for the proper administration of justice. See also *Toth v City of Niagara Falls*, 2017 ONSC 5670 (CanLII) [*Toth*], where the Court held that documents relevant to the Plaintiff's case on the public Facebook page of a non-party should have been disclosed by the Plaintiff.

200. See *Dosanjh v Leblanc* 2011 BCSC 1660 (CanLII) [*Dosanjh*].

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

obtained in the discovery process, and it specifically does not apply to evidence filed with the court or referenced during a hearing. A court order can also be obtained to relieve a party from compliance with the deemed undertaking rule.[202]

Violation of these undertakings may give rise to a privacy-based cause of action for the individual whose personal information was compromised as a result of the violation. Parties should therefore ensure that appropriate controls are placed on the access and retention of information gained through the discovery process.

Guidelines regarding privacy and information security for legal service providers have been published by Sedona Canada. They focus on the regulatory and practice requirements of the Canadian legal profession. *The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers*[203] sets forth six guiding principles examining applicable ethical rules and statutory obligations and providing concrete guidance relating to privacy and information security for legal service providers.

In 2018, the General Data Protection Regulation[204] became applicable to members of the European Union (EU). The regulation seeks to harmonize data privacy laws by imposing privacy protection requirements for personal information both within and flowing out of the EU. The GDPR provides protections related to the preservation, collection, use, and transfer of EU citizens' data. These protections are also applicable to data transferred outside of the EU. The GDPR is just one example of an international privacy regime that could affect the disclosure

202. *Ontario Rules of Civil Procedure*, r 30.1.01.

203. "Sedona Canada Commentary on Privacy and Information Security," *supra* note 69.

204. GDPR, *supra* note 72.

of documents in Canadian litigation. Counsel should ensure to familiarize themselves with the privacy regimes, both domestic and international, that are potentially applicable to their case. Consultation regarding foreign privacy laws is essential when dealing with multinational organizations or cross-border matters involving data outside of Canada.

Comment 9.c.i. Social Media

A party must consider whether social media content and documents are relevant and should be preserved and listed in an affidavit or list of documents or records.[205] 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 and the burden of production.[206] 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.[207] Rather, relevance must be shown. For example, in *Bishop v. Minichiello*, the defendants sought production of the plaintiff's hard drive to determine the amount of time the plaintiff spent on Facebook.[208]

---

205. *Toth*, *supra* note 199, where the Court found that counsel for the plaintiff, should have considered the existence of social media content in a public forum (i.e., Facebook).

206. 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); *Casco v Greenhalgh*, 2014 CarswellOnt 2543 (Master); *Papamichalopoulos v Greenwood*, 2018 ONSC 2743 (CanLII) and *Wilder v Munro*, 2015 BCSC 183 (CanLII).

207. *Schuster v Royal & Sun Alliance Insurance Company of Canada*, 2009 CanLII 58971 (ON SC); *Stewart v Kemptster*, 2012 ONSC 7236 (CanLII); *Garacci v Ross*, 2013 ONSC 5627 (CanLII), and *Conrod v Caverley*, 2014 NSSC 35 (CanLII).

208. *Bishop v Minichiello*, 2009 BCSC 358 (CanLII), leave to appeal for further production dismissed *Bishop v Minichiello*, 2009 BCCA 555 (CanLII).

The plaintiff's computer was used by all members of his family. To protect the privacy rights of non-party family members, the Court ordered the parties to agree on the use of an independent expert to review the hard drive. In *Fric v. Gershman*,[209] 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, 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.[210] Although the presence of relevant information on the public portion of a party's social media page may support the inference that relevant information is also contained in the party's private profile, courts have held that in some circumstances, users have a privacy interest in the information that they have chosen not to share publicly.[211]

Even where individuals seek to operate under the privacy that may be afforded by the anonymity of social media profiles, there will be instances where the court determines that the public interest and fairness override an individual's expectation of anonymity and privacy. In *Olsen v. Facebook,*[212] the Court held that anonymous posters should not be permitted to defame without consequences. However, individuals who comment on matters of public interest should not have their anonymity stripped away when they are critical of public figures.

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

210. *Ibid* at para 75, citing *Dosanjh*, *supra* note 200.

211. *Jones v IF Propco*, 2018 ONSC 23 [*Jones*].

212. *Olsen v Facebook*, 2016 NSSC 155.

Ultimately, the Court found the nature and number of postings by the Facebook accounts overrode a reasonable expectation that account owners were entitled to anonymity, and the Court ordered Facebook to release to the applicants the preserved Facebook information.

Where possible, social media content should be collected and produced in a forensically sound manner; screen captures and printed paper versions may be unreliable,[213] and therefore inadmissible.

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 provider 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 emailing or "friending" that party, this may violate the no-contact rule.

Comment 9.c.ii. Privacy issues and Ephemeral Messaging

Ephemeral messaging is technology that allows users to send *temporary* text messages, pictures, or other electronic communications, which self-delete after a period of time or after the message is viewed by the recipient (see discussion above in Principle 6). In some instances, the communication is encrypted, although that is not always the case. As in the case of social media content, a party has a legal obligation to preserve and produce ephemeral messages when such messages are or may be

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

relevant to litigation. In *Uber v. Waymo,*[214] Waymo was permitted to present evidence to demonstrate that Uber was using an ephemeral messaging app to deliberately conceal evidence relating to theft of Waymo's trade secrets. The case was settled shortly after the trial began, thus ending any further disclosure of information relating to Uber's use of ephemeral messaging.

There is little case law to date discussing ephemeral messaging. The question of whether the privacy interest in such messages is any different from other social media content has not yet been considered. However, the very nature of ephemeral messaging apps suggests that there may be an even higher bar to override a person's expectation of privacy in these types of messages. These apps were designed specifically with privacy in mind by having messages quickly self-destruct, thus mimicking a live conversation and avoiding a permanent record. By the same token, the use of encrypted private messaging apps may also be more likely to engage a reasonable expectation of privacy.

Guidance on this issue may be found in *R v. Marakah*,[215] where the Supreme Court of Canada found that text messages that have been sent and received may be protected under Section 8 of the *Canadian Charter of Rights and Freedoms* ("Charter").[216] Whether such reasonable expectation of privacy exists, however, will depend on the particular facts of the case.

---

214. *Waymo LLC v Uber Technologies, Inc.*, No. C 17-00939 WHA (N.D. Cal. Jun. 8, 2017).

215. *R v Marakah,* 2017 SCC 59 [*Marakah*].

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

Comment 9.c.iii. 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.[217] The Court held that employees may have a reasonable expectation of privacy where personal use is permitted or reasonably expected. Ownership of the device 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.*,[218] the Labour Relations Board held that if an employee chooses to use a company vehicle for transportation to and from home, the company is not restricted from using technological devices to monitor the vehicle at all times.

In *Greenhalgh v. Verwey,*[219] the Court held that an expectation of privacy on a company-owned computer is reduced. The Court concluded that the evidence resulting from the applicant's search of a hard drive on an abandoned company computer should be admitted. In the recent labour arbitration award *Canadian Broadcasting Corporation v. Canadian Media Guild*, the arbitrator held that a temporary employee had a reasonable expectation of privacy in WhatsApp messages sent from a shared work computer.[220]

---

217. *Ibid*.

218. *Elevator Constructors Union*, *supra* note 213.

219. *Greenhalgh v Verwey,* 2018 ONSC 3535 (CanLII).

220. *Canadian Broadcasting Corporation v Canadian Media Guild*, 2021 CanLII 761 (CA LA).

In contrast 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 "bring your own device" or "BYOD"). Many organizations acknowledge and accept the use by employees of employee-owned digital devices on corporate networks. If employees are using their own devices, BYOD policies are essential for the employer to gain access to the device for discovery purposes.

Generally, BYOD policies or agreements indicate that the employee retains ownership of the device, while the employer retains ownership and control of business-related communications and the professional work product created or maintained on the device. Employers should ensure that their BYOD policy clearly defines the relationship between the employee, employer, and the device. The policy or agreement should specifically address scenarios where the employer may require and is permitted access to the device for legitimate work purposes, including but not limited to discovery.

Comment 9.c.iv. 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 from unreasonable search or seizure under section 8 of the Charter.

As discussed above, the Supreme Court of Canada in *R v. Marakah*[221] found that text messages that have been sent and received may be protected under Section 8 of the Charter. In that case, the accused in a criminal proceeding had a reasonable

221. *Marakah*, *supra* note 215; *Jones*, *supra* note 211.

expectation of privacy in text messages recovered from the phone of the accused's accomplice.

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*[222] should be applied to obtain the appropriate court orders and protections, as required. Prior to the release of criminal investigatory materials, 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, service providers, 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 other parties.

Safeguards should be put in place to address privacy compliance, cybersecurity, and IT services that manage the organization's data. *The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines*[223] identifies policies and practice considerations to address such privacy and security obligations, including personal, confidential, and privileged information. The *Commentary* provides six guiding principles for legal service providers

222. *D. P. v Wagg*, 2004 CanLII 39048 (ON CA) [*Wagg*].

223. "Sedona Canada Commentary on Privacy and Information Security," *supra* note 69.

to consider in order to protect personal and confidential information:

- Principle 1: Know the law;
- Principle 2: Understand the personal and confidential information you control;
- Principle 3: Assess risk;
- Principle 4: Develop policies and practices;
- Principle 5: Monitor regularly; and
- Principle 6: Reassess.

In the context of discovery, the protection of client data and other parties' data should 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, as well as appropriate procedures for disposition after the conclusion of a matter or engagement.

Appropriate chain-of-custody logs and procedures should be used to maintain the integrity of the data from collection to use 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 matter.

At a minimum, data should be password-protected, preferably through two-factor authentication.[224] Hackers have frequently targeted law firms and may view them as soft targets. In addition to ensuring technological security, access should be

224. 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 personal identification number.

restricted to those with a "need to know," and both physical storage facilities and computer servers should be secured from unauthorized access.

Law firms or legal departments involved in the vetting and selection of litigation support technologies and/or third-party service providers should adequately review cybersecurity risks and vulnerabilities, including periodically auditing and reassessing them.

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 within the same jurisdiction (e.g., civil court, criminal court, arbitration, administrative, or regulatory hearing) or in different jurisdictions (e.g., local, provincial, federal, and other nations such as the U.S., countries in Europe, and elsewhere). Whether within a single jurisdiction or between jurisdictions, 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.

In any proceeding, counsel must comply with specific discovery rules applicable to the particular forum or jurisdiction. Counsel needs 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 Québec[225] differs from discovery processes in the common law

225. See *Québec Code of Civil Procedure*.

provinces. For example, in Ontario,[226] "relevant" documents must be produced, whereas in Alberta,[227] "relevant and material" documents must be produced. Different still is British Columbia,[228] which requires the disclosure of documents that could be used at trial to prove a material fact and all other documents that a party intends to refer to at trial.

Many provinces do not address the production of electronic evidence specifically in their rules of court. However, Nova Scotia's discovery rules provide meaningful guidance on electronic evidence, including commentary on preservation, when ESI is considered in a party's control, and a default rule respecting what constitutes a sufficient search of ESI absent a discovery agreement between parties.[229] The court rules in Saskatchewan[230] and Manitoba[231] reference a Practice Directive that sets out guidelines for the discovery of electronic evidence that in many respects mirror these *Principles.* The Ontario *Rules of Civil Procedure* specifically reference the *Sedona Canada Principles* and direct parties to consult them.

Counsel should be aware of the procedural and substantive differences in the discovery process, and in the privilege, privacy, and evidence rules between Canada and the United States, as well as between North American jurisdictions and those in Europe.

---

226. *Ontario Rules of Civil Procedure*, rule 30.02.

227. *Alberta Rules of Court*, rule 5.6.

228. *Supreme Court Civil Rules*, rule 7-1.

229. *Nova Scotia Civil Procedure Rules*, rule 16

230. Court of Queen's Bench for Saskatchewan, Practice Directive No 1 (E-Discovery Guidelines).

231. Court of Queen's Bench of Manitoba, Guidelines Regarding Discovery of Electronic Documents.

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 be vigilant in ensuring that clients are not compromised in one forum or jurisdiction by actions taken in another. This may involve engaging counsel from other jurisdictions.

Any possible conflicts between the rules in different forums should be identified early and mitigated to the extent required.

In multijurisdictional litigation, parties should attempt to align their discovery processes while taking into account local rules and production obligations. For example, it may be more cost-efficient for a client to reproduce any documents they have produced in a U.S. class action where a similar or parallel proceeding is started in Canada.

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 matter:

1. **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.
2. **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.

3. **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 third-party "cloud" service providers, 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.

4. **Affidavit or Certification.** The responsibility for swearing or certifying the completeness of the collection of documents produced in the proceeding, as well as the language used to attest to the undertaking, 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.

5. **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.

6. **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.

7. **Privacy, Confidentiality, and Data Transfer Prohibitions.** Privacy laws vary between jurisdictions. Europe, in particular, has enacted stringent and wide-sweeping privacy laws that strictly regulate the collection, use, and transfer of personal information. The GDPR limits the transfer of data outside the European Union in many circumstances, including possible transfers in respect of a foreign legal proceeding. It has also made consent by the data owner to the use and transmission of its personal data a less reliable exception to the GDPR's prohibitions. The GDRP has only recently come into force, and as such the interpretation of its provisions is limited. Practitioners dealing with clients who have European operations or employees would be wise to consult European legal counsel with a knowledge of European privacy law if they expect to need to disclose any information stored in Europe or created or maintained by a European citizen.

   There are other jurisdictions that prohibit the transfer outside of their borders of certain types

of information, sometimes referred to as "data localization laws." Moreover, many countries limit the transfer of information they consider vital for their defence and national security.

8. **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) vary in foreign jurisdictions. For example, certain jurisdictions in the United States do not recognize a common-interest protection for shared lawyer-client communications in the context of a business transaction. While this type of privilege protection is recognized in Canada,[232] it may have limited application in New York,[233] for example. To the extent counsel on different sides of the border are reviewing documentation for privilege in cross-border litigation, it will be necessary to coordinate the approach to privilege claims being made, considering the differences in laws.

   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

232. *Iggillis Holdings Inc. v Canada (Nation Revenue),* 2018 FCA 51 (CanLII) (leave to appeal to SCC denied).

233. *Ambac Assurance Corp. v Countrywide Home Loans*, Op. No. 80, 57 N.E. 3d 30 (NY 2016).

rules so as not to inadvertently waive privilege in another jurisdiction.

9. **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.

10. **Specific eDiscovery 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 can 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.[234]

234. 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

The Sedona Conference International Overview of Discovery, Data Privacy and Disclosure Requirements provides an overview of discovery and data privacy laws in a number of countries around the world.[235]

Comment 10.b. Forums

Different procedural and substantive laws can 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 be cognizant of the impact its decisions respecting the collection, review, and production of data in one forum could have on the disclosure of evidence in another. For example, in the case of a bankruptcy proceeding in which there are allegations of criminal wrongdoing against the bankrupt and its employees, officers, or directors, the trustee in bankruptcy should consider appropriate protections (e.g., the giving of advance notice to affected parties) before delivering documents to a law enforcement agency or

---

Sedona Conference <https://thesedonaconference.org/publication/The_Sedona_Canada_Commentary_on_Enforcing_Letters_Rogatory_Issued_By_an_American_Court_in_Canada>.

235. The Sedona Conference, "International Overview of Discovery Data Privacy and Disclosure Requirements" (2009), online: The Sedona Conference <https://thesedonaconference.org/publication/International_Overview_of_Discovery_Data_Privacy_and_Disclosure_Requirements>.

regulator that are protected by privilege in favour of an individual who is not the bankrupt.

Counsel should ensure appropriate protective 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, as will efforts, where it is in the client's interests, to harmonize discovery requirements in the different forums.

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 Charter and an accused's right to a fair trial.[236] Where electronic evidence has been seized, warrants and various search and seizure provisions of the Criminal Code can be implicated.[237]

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

---

236. *Kelly v Ontario*, 2008 CanLII 22557 (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).

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

investigation, prior to use or disclosure in any other proceeding, the principles and screening process identified in *D.P. v. Wagg*[238] should be applied to obtain the appropriate court orders to protect, as necessary, privacy rights and privilege rights.[239] Prior to the disclosure 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.[240]

Regulatory bodies also have the ability to compel the production of evidence through enforcement provisions in the governing legislation.[241] In addition to the power to compel, the regulatory body may have the power to control subsequent disclosure and use of the compelled evidence.[242] 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

---

238. *Wagg*, *supra* note 222; Generally, the deemed undertaking rule prohibits parties from disclosing evidence and information obtained during the discovery process outside the confines of the litigation.

239. The need to obtain consent of the Crown is also required in parallel regulatory proceedings, even where the regulatory body has the statutory ability to compel evidence. See *College of Physician and Surgeons of Ontario v Peel Regional Police*, 2009 CanLII 55315 (ON SCDC).

240. 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.

241. 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.

242. For example, Ontario *Securities Act,* RSO 1990, c S.5, s 16-18, and BC *Securities Act*, RSBC, c 418, s 148 give the respective Commissions the ability to limit and place restrictions on the subsequent disclosure or use of the seized evidence; *Cole*, *supra* note 216.

opportunity to raise public interest concerns that may militate against production.[243]

Matters that involve cross-border criminal or regulatory proceedings require particular consideration of the different 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,[244] 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.[245]

Comment 10.b.ii. Arbitration

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

Subject to the rules specified in the arbitration agreement, parties are typically required to produce only the documents upon which they rely 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 ADR Institute of Canada's *ADRIC Arbitration Rules* ("ADRIC Rules").[246] Rule 4.13 of the ADRIC Rules outlines a useful framework for producing and requesting documents and resolving any disputes that may arise. An alternative, but

---

243. *College of Physicians and Surgeons of Ontario v Metcalf*, 2009 CanLII 55315 (ON SCDC), see paras 68–77.

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

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

246. *ADRIC Arbitration Rules*.

similar, framework can be found in Article 3 of the International Bar Associate's *Rules on the Taking of Evidence in International Arbitration*.[247] The ADRIC Rules provide for the parties to produce lists of those documents available to them and upon which they rely. A party may also deliver to any other party a request to produce, which must identify the requested documents, or a narrow category of documents, and explain how they are "relevant to the case and material to its outcome."[248] A party that objects to producing the requested documents must communicate its objection to the tribunal. The ADRIC Rules list several justifiable objections to production, including lack of sufficient relevance or materiality, legal privilege, and unreasonable burden.

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.[249] Fortunately, the flexibility that is inherent in the arbitral process, if harnessed by counsel and arbitrators, may assist in managing the issue more effectively. Concerns around reasonable and narrow document production are also reflected in the ADRIC Rules, particularly Rule 4.13.4(a)(ii), which requires that where a request seeks electronic documents, "the requesting party must identify specific files, search terms, individuals, or other means of searching for the Documents efficiently and economically."

Parties engaged in arbitration proceedings should be aware that while the scope of their production obligation may be more limited, the work undertaken to fulfill it may not be. Unless the

---

247. IBA Rules on the Taking of Evidence in International Arbitration (29 May 2010), online: International Bar Association.

248. *ADRIC Arbitration Rules* at r 4.13.4.

249. Richard D. Hill, "The New Reality of Electronic Document Production in International Arbitration: A Catalyst for Convergence?," *Electronic Disclosure in International Arbitration* (2008) 25:1 Arb.

client has a good handle on the case, in particular as to which documents will be relevant and where they are stored, it may still be necessary to do a comprehensive document collection and review. It may also 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 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 may be appropriate 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, reckless, or negligent destruction or nonproduction 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.

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, parties may fail to fully preserve or disclose all relevant material. In considering the appropriate sanction for nondisclosure or destruction of ESI, the court may consider the context, scope, and impact of the nondisclosure. More particularly, the following factors are relevant: the level of culpability of the party, the intention or reason behind the destruction or nonproduction, the sophistication of the party in handling ESI, the party's retention policies, whether primarily prejudicial documents have been destroyed, the costs and burden involved in efforts that could have preserved the documents in question, the prejudice to the requesting party, and the impact that the loss of ESI may have on the court's ability to fairly dispose of the issues in dispute.

Comment 11.a. The Tort of Spoliation

Whether spoliation exists as an independent tort in Canada is an open question.[250]

Although the British Columbia Court of Appeal held in *Endean v. Canadian Red Cross Society*[251] that spoliation would not ground an independent tort, other courts have refused to strike allegations of the tort of spoliation in pleadings.[252]

In *Spasic (Estate) v. Imperial Tobacco Ltd.*, 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

250. *Spasic*, *supra* note 58 (leave to appeal to SCC denied).

251. *Endean v Canadian Red Cross Society*, 1998 CanLII 6489 (BC CA) [*Endean*] at paras 9, 20–34.

252. *Spasic*, *supra* note 58 at paras 15–26; *Cummings v MacKay*, 2003 NSSC 196 at paras 15–16 (CanLII), aff'd 2004 NSCA 58 at para 9 (CanLII); *Kacperski v Orozco*, 2005 ABCA 179 at paras 4–9 (CanLII), but see *Logan*, *supra* note 111 at paras 41–42.

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 and that the claims pleaded should be allowed to proceed to trial, as the few Canadian cases that have considered the issue were not definitive.

In *Western Tank & Lining Ltd. v. Skrobutan et al*,[253] the Court concluded that "acts of spoliation can constitute an independent tort" but resolved the spoliation issue in the case by drawing a negative inference instead of awarding damages.[254] In *CMT et al v. Government of PEI et al*,[255] the Court considered the evidence in light of the elements of the tort of spoliation but found that the tort had not been made out.[256]

Some commentators have advocated for a tort of spoliation. For example, in 2004, the British Columbia Law Institute concluded that the creation of the independent tort of spoliation will fill several gaps in the law.[257]

Comment 11.b. Spoliation as a Rule of Evidence

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

253. *Western Tank & Lining Ltd. v Skrobutan et al*, 2006 MBQB 205 (CanLII) [*Western Tank*].

254. *Ibid*; *Canada Evidence Act*, RSC 1985, c C-5, s 31.8. [*Canada Evidence Act*], para 22.

255. *CMT et al v Government of PEI et al*, 2019 PESC 40 (CanLII).

256. *Ibid* at paras 608, 635–39.

257. British Columbia Law Institute, *Report on Spoliation of Evidence*, BCLI Report No. 34 (November 2014), pp 36–46, online: <http://www.bcli.org/sites/default/files/Spoliation_of_Evidence_Rep.pdf>.

permits a court to draw a negative inference against a party that has been guilty of destroying or suppressing evidence.[258]

The most comprehensive review of the Canadian jurisprudence on the common law of spoliation is found in *McDougall v. Black and Decker Canada Inc*.[259] 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.[260]
- 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.

---

258. *Zahab v Salvation Army in Canada,* 2008 CanLII 41827 (ON SC), at para 20, citing *Prentiss v Brennan*, [1850] OJ No 283 (Upper Canada Court of Chancery). But see *Gladding Estate v Cote*, 2009 CanLII 72079 (ON SC) at para 36: The court will only draw a negative inference where there is "real and clear evidence of tampering."

259. *McDougall*, *supra* note 58.

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

- 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 as part of the law of negligence, 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.

More recently, in *Nova Growth Corp. v. Andrzej Roman Kepinski*,[261] the Court concluded that a finding of spoliation requires four elements to be established on a balance of probabilities:

1. The missing evidence must be relevant;
2. The missing evidence must have been destroyed intentionally;
3. At the time of destruction, litigation must have been ongoing or contemplated; and

261. *Nova Growth Corp. et al v Andrzej Roman Kepinski et al*, 2014 ONSC 2763 (CanLII).

4. It must be reasonable to infer that the evidence was destroyed in order to affect the outcome of the litigation.

A party is not typically required to plead spoliation to rely on it as a rule of evidence.[262] However, it may be prudent for a party to provide notice to the alleged spoliator before raising the issue of spoliation at trial. In the context of the destruction of the ESI specifically, the alleged spoliator may be able to obtain lost evidence by going above and beyond what is ordinarily required, e.g., by recovering deleted files or obtaining ESI from a third party.

There is limited guidance specifically dealing with spoliation in the rules of court across the various provinces. In Nova Scotia, however, the *Civil Procedure Rules* have been amended to include provisions that expressly deal with the duties to preserve and disclose electronic information, and the consequences of their breach.[263]

Comment 11.c. Negligent Destruction of Evidence

In *McDougall v. Black & Decker Canada Inc.*,[264] the Alberta Court of Appeal distinguished spoliation of evidence—being

262. *Spasic*, *supra* note 58 at para 25 (leave to appeal to SCC denied); *Blais*, *supra* note 260 at para 85.

263. The Nova Scotia *Civil Procedure Rules* 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.

264. *McDougall*, *supra* note 58.

intentional destruction of evidence[265]—from *negligent/reckless* destruction. In the latter case, the Court concluded, it was "not appropriate to apply the presumption that the evidence would tell against the spoliator when evidence has been lost or destroyed carelessly or negligently."[266] However, "where that evidence [was] not intentionally destroyed, but destroyed through negligence, [remedies] may arise from the procedural rules of court, a trial judge's discretion on matters of costs and his or her duty to control abuse of process."[267]

In the development of retention periods in the context of information governance policies, parties should consider the impact of automatic deletion/disposal processes to ensure the approaches they are taking is legally defensible.

Comment 11.d. Sanctions for Spoliation

Canadian jurisprudence regarding the appropriate response to the destruction of ESI is relatively limited but developing.[268] 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

---

265. See *Chow-Hidasi v Hidasi*, 2013 BCCA 73 (CanLII) at para 29, which confirms that spoliation requires intentional conduct (with "intentional" defined as "knowledge that the evidence would be required for litigation purposes").

266. *McDougall*, *supra* note 58 at para 24.

267. *Ibid* at para 22.

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

awarded, the facts show either intentional conduct or indicate that a party or the administration of justice will be prejudiced in the preparation of the case for trial.[269]

The most severe penalty imposed by a Canadian court for spoliation was in *Brandon Heating and Plumbing (1972) Ltd. et al v. Max Systems Inc.*,[270] where the plaintiff provided undertakings to preserve certain hardware, disks, and documents, as they were key to the defendant's defense. Instead, 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.

Findings of the spoliation of evidence have resulted in the following pretrial remedies:

1. Drawing an adverse inference in the context of an interlocutory application[271]
2. Prohibition of the use (at trial) of any reports or other evidence that relates to the destroyed evidence[272]
3. Prohibition of the use (at trial) of evidence subsequently located;[273]
4. Examination of the expert, expert's notes, and photographs[274]

---

269. *Cheung v Toyota*, 2003 CanLII 9439 (ON SC) [*Cheung*]; *Western Tank*, *supra* note 253.

270. *Brandon Heating & Plumbing (1972) Ltd. et al v Max Systems Inc.*, 2006 MBQB 90 (CanLII) [*Brandon Heating*].

271. *Western Tank*, *supra* note 253.

272. *Cheung*, *supra* note 269 at para 31.

273. *Jay v DHL*, 2009 PECA 2 at para 73(a) (CanLII).

274. *McDougall*, *supra* note 58 at para 39.

5. Civil contempt (if destruction is done in breach of an order)[275]
6. Additional examinations for discoveries[276]
7. Dismissal of the claim[277]

At trial, the courts have also granted the following remedies:

1. Drawing an adverse inference[278]
2. Depriving the successful party of costs[279]
3. Special costs[280]
4. Exclusion of an expert report[281]

Furthermore, courts in some jurisdictions have authority to impose sanctions if the parties fail to agree to a discovery plan or have failed to update a discovery plan. For example, in Ontario the court may refuse to grant any discovery-related relief or to award any costs.[282]

In other jurisdictions, the failure to reach agreement results in a reversion to default provisions. In Nova Scotia, Rule 16 of the *Civil Procedure Rules* contemplates the possibility that the parties might reach agreement regarding certain electronic disclosure issues. Absent such an agreement, the *Civil Procedure*

---

275. *Fuller Western Rubber Linings Ltd. v Spence Corrosion Services Ltd*., 2012 ABQB 163 at para 41 (CanLII).

276. *Apotex Inc. v H. Lundbeck A/S*, 2011 FC 88 at paras 34–37 (CanLII).

277. *Brandon Heating*, *supra* note 270 at para 33.

278. *Forsey v Burin Peninsula Marine Service Centre*, 2014 FC 974 at para 124 (CanLII); *Elsen v Elsen*, 2010 BCSC 1830 at para 330 (CanLII); *Trans North Turbo Air Ltd. et al v North 60 Petro Ltd. et al*, 2003 YKSC 18 at para 84 (CanLII).

279. *Farro v Nutone Electrical Ltd.,* 1990 CanLII 6775 (ON CA).

280. *Endean*, *supra* note 251 at para 33.

281. *Ibid* at para 32; *Roe v Warner Auto Mechanic*, 1996 CanLII 925 (ON CA); *Dyk v Protec Automotive Repairs Ltd*., 1997 CarswellBC 1872 (BCSC).

282. Ontario *Rules of Civil Procedure,* r 29.1.05; *TELUS*, *supra* note 117; *Petrasovic*, *supra* note 104.

Rules set out various default provisions which are to apply.[283] In Saskatchewan, the *Civil Practice Directive* governing eDiscovery states that the parties should confer and attempt to agree on issues relating to eDiscovery. Where parties are unable to agree on issues surrounding the use of technology for the preparation and management of litigation, the default standard is specified in the Canadian Judicial Council's *National Generic Protocol on the Use of Technology in Civil Litigation*.[284]

Comment 11.e. Rebutting the Presumption of Spoliation

No formal exemption or defense against spoliation exists in Canadian court rules.[285] 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 that favour sanctions.[286]

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

---

283. Nova Scotia *Civil Procedure Rules*, rule 16.

284. Court of Queen's Bench, *Practice Directives, Civil Practice Directive No. 1 E-Discovery Guidelines*, Effective: July 1, 2013, Saskatchewan.

285. Until 2015, there was a formal "safe harbor" under Rule 37(e) of the U.S. Federal Rules of Civil Procedure, which provided 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. The Rule was substantially modified in 2015 to require parties to take reasonable steps to preserve ESI that "should have been preserved."

286. *Leon v Toronto Transit Commission,* 2014 ONSC 1600 (CanLII); *Stilwell*, *supra* note 260.

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 would not have been retained (and for how long) is helpful."[287] 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.[288] In contrast, courts have been willing to draw adverse inferences in circumstances where the failure to produce a document is tied to either the destruction of a document through an ad hoc procedure[289] or an unreasonably short retention policy.[290]

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. To determine admissibility of digitized electronic records in lieu of paper originals, some jurisdictions permit evidence to be presented regarding standards and best practices

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

288. *Stevens v Toronto Police Services Board*, 2003 CanLII 25453 (ON SC). See also *Moutsios c Bank of Nova Scotia*, 2011 QCCS 496 (CanLII) 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.

289. *Moezzam Saeed Alvi v YM Inc.*, 2003 CanLII 15159 (ON SC); *Ontario v Johnson Controls Ltd*., 2002 CanLII 14053 (ON SC).

290. *Moezzam Saeed Alvi v YM Inc. (sales)*, 2003 CanLII 15159 (ON SC) at para 48; *Ontario v Johnson Controls Ltd*., 2002 CanLII 14053 (ON SC) at paras 50–51.

used by organizations and applied to the creation and storage of the digitized records.[291]

Similar considerations arise when technological limitations make production of certain file types unnecessarily costly or impossible, e.g., extraction of emails from outdated systems, or redaction of complex drawings and spreadsheets. In such instances, the parties may agree that the production of files in a different format (e.g., PDF) is adequate as long as sufficient indicia of reliability are present.

It is important to distinguish the courts' approach to sanctions for spoliation from their approach to sanctions for breaching a court order. The factors for determining the appropriate sanction for failure to comply with the obligations to disclose documents (or for other similar failures) were considered in *Zelenski v. Jamz.* [292] The Court held it was appropriate to take into account such factors as: (1) the quantity and quality of the

---

291. 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, s 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*, RSNS, 1989, c 154 by *Saturley v CIBC World Markets Inc.,* 2012 NSSC 226 (CanLII). These standards are not mandatory. Some common standards in use by organizations include: the Canadian General Standards Board, online: Public Services and Procurement Canada; Standards Council of Canada, CAN/CGSB 72.34-2005 Electronic Records as Documentary Evidence, online: Standards Council of Canada; Standards Council of Canada, Microfilm and Electronic Images as Documentary Evidence (CAN/CGSB-72.11-93 as amended 2000), online: Standards Council of Canada; International Organization for Standardization (ISO), ISO/CD 15489-1 Information and Documentation Records Management, online: ISO; and ARMA International's Generally Accepted Recordkeeping Principles, online: ARMA.

292. *Zelenski v Zelenski*, 2004 MBQB 256 at para 19 (CanLII), aff'd *Zelenski v Jamz,* 2005 MBCA 54 (CanLII).

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.

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.

Comment 12.a. Interim Cost Shifting

In most Canadian provinces and territories, the costs of discovery are traditionally borne by the producing party at the time they are incurred, with any shifting of costs potentially occurring at the end of the litigation, at which time an unsuccessful party may be required to contribute, in whole or in part, toward the costs (fees and disbursements) of the successful party. This contribution generally includes the allocation of the costs of producing ESI during the discovery phase of the litigation.[293]

293. 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 <https://www.bccourts.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*

In Canada, a court is empowered to order that the costs of producing ESI be shifted to a party other than the producing party at any time in the litigation. Such cost shifting, however, does not often occur in Canadian jurisprudence. Often the mention of a cost-shifting motion brings both parties to the table, where they can discuss a proportionate approach to the scope of discovery.

For the most part, courts still continue to follow the traditional rules and refuse to shift the costs of production of ESI at the discovery stage. In *Gamble v. MGI Securities*,[294] the Court ordered the defendant to deliver its productions in CSV[295] format and refused to shift the costs of doing so to the plaintiff. In doing so, the Court did consider *The Sedona Canada Principles* and the disparity in the parties' abilities to pay for production. Similarly,

---

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 traditional approach to discovery costs. See also *Bank of Montreal v 3D Properties,* 1993 CanLII 8918 (SK QB) at para 30: "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."

294. *Gamble*, *supra* note 174.

295. CSV: Comma Separated Value. See "Sedona Conference Glossary," *supra* note 1 at 281.

in *GRI Simulations Inc. v. Oceaneering International Inc.*,[296] 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.

In deciding whether to make an order on an interim basis shifting the costs of production of ESI from the party producing the evidence to another party, it is appropriate to consider the following (nonexhaustive) list of factors:

1. The existence of an attempt by one or more of the parties to engage the other party or parties in a negotiation for a discovery plan
2. The importance of the evidence sought to be disclosed by the producing party to the case, and the impact on any party of not getting access to the information sought
3. The burden on, and costs to, the producing party to identify, collect, review, and/or produce the requested ESI, and that party's ability to bear the costs and or burden
4. The accessibility of the ESI sought
5. The efforts the parties made to find a creative or cost-efficient solution to the discovery request at issue
6. If applicable, whether the producing party can avail itself of newer technology or methodologies to reduce costs (such as technology-assisted review/continuous active learning)
7. The refusal of any party to agree to cost-saving measures, for example, confidentiality or

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

clawback provisions that may limit the need to perform more extensive and costly legal review

8. The extent to which a request to produce ESI is as tailored as possible to discover relevant ESI
9. The producing party's failure to produce relevant ESI that seems likely to have existed but is no longer available on more readily accessible sources, and the reasons for that lack of availability
10. The total cost of production (including the estimated costs of processing and reviewing retrieved documents), compared with the amount in dispute in the litigation

A good example of where cost shifting might be appropriate on an interim basis is when extraordinary effort or resources will be required to restore old, archived data to an accessible format (e.g., accessing disaster recovery media, 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 it may be unfair and may limit the party's resources to litigate the dispute on the merits. Accordingly, it may be appropriate that the party requesting such extraordinary efforts bear, at least on an interim basis, all or part of the costs of doing so.

Additionally, eDiscovery 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 set out in the various court rules across the country 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

should now be considered a standard disbursement.[297] These costs could also, therefore, be subject to a cost-shifting order.

Comment 12.b. Conduct During Discovery and Cost Awards

The parties' conduct during the discovery phase of litigation should inform costs awards. For example, requirements around discovery plans may impact the costs a court will award.

In *Koolatron v. Synergex,*[298] the producing party failed to produce several records agreed to in undertakings. Although the receiving party was successful in its motion and would have been entitled to costs, its failure to create a discovery plan to set out an efficient process for production meant no costs were awarded.

In *LTS Infrastructure v. Rohl et al,*[299] a producing party agreed to objectively code records in a document exchange protocol. When the parties exchanged their documents "a significant amount ha[d] incorrect document dates." The Court agreed that 100 percent accuracy is impractical, but due to the party's agreement to objectively code the documents in the exchange protocol, the plaintiff was responsible for the costs associated with correcting the errors.

Parties that cause an unreasonable burden on opposing parties by producing a voluminous number of documents with little to no culling of irrelevant data may also be penalized. In *Manchanda v. Thethi*[300] the Court stated: "I am referring to an abusive, old-school practice whereby a party discloses a large number of disorganized documents so as to inflict cost and

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

298. *Koolatron v Synergex*, 2017 ONSC 4245 (CanLII).

299. *LTS Infrastructure*, *supra* note 142.

300. *Manchanda v Thethi*, 2016 ONSC 3776 (CanLII).

confusion for the receiving party. Apart from imposing a significant time burden on the receiving party by requiring counsel to organize the documents, a document dump can also be a way to try to hide damaging documents. Damaging documents can be located among a load of irrelevant ones to try to deprive the harmful documents of context." The Court ordered substantial indemnity costs against the respondent, in part for this behaviour.

As eDiscovery costs are often significant, and given that cost shifting occurs relatively infrequently, parties must make good-faith efforts to adopt strategies to control the costs of eDiscovery. It may be unfair that a losing party in litigation should have to pay for discovery done poorly, inefficiently, or in a manner that needlessly increased costs, even if the party was ultimately unsuccessful in the case. The producing parties should take advantage of technology that enables them to be more efficient in the discovery process, such as machine learning in document review. In *The Commissioner of Competition v. Live Nation Entertainment, Inc et al,*[301] the Competition Tribunal specifically encouraged "the use of modern tools to assist in these document-heavy cases where they are as or more effective and efficient than the usual method of document collection review." Similarly, in *Cass v. 1410088 Ontario Inc.*,[302] the Court rejected an order for costs on the basis that "[i]f artificial intelligence sources were employed, no doubt counsel's preparation time would have been significantly reduced."

301. *Live Nation*, *supra* note 189.

302. *Cass v 1410088 Ontario Inc.*, 2018 ONSC 6959 (CanLII).