The Sedona Conference Journal®

Volume 23 ❖ 2022 ❖ Number One

Articles

Antitrust Law, Complex Litigation, Intellectual Property Rights, and Data Security and Privacy Law

The Sedona Conference Journal®

Volume 23

■

2022

Number 1

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual or semi-annual basis, containing selections from the preceding year's conferences and Working Group efforts. A PDF copy of The Journal is available on a complimentary basis and can be downloaded from the Publications page on The Sedona Conference website: www.thesedonaconference.org. Check our website for further information about our conferences, Working Groups, and publications.

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

The Sedona Conference Journal® cover designed by MargoBDesignLLC at www.margobdesign.com.

Cite items in this volume to "23 Sedona Conf. J. _____ (2022)."

Publisher's Note

Welcome to Volume 23, Number 1, of The Sedona Conference Journal (ISSN 1530-4981), published by The Sedona Conference, a nonprofit 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way through the creation and publication of nonpartisan consensus commentaries and advanced legal education for the bench and bar.

The various Working Groups in The Sedona Conference Working Group Series (WGS) pursue in-depth study of tipping-point issues, with the goal of producing high-quality, nonpartisan consensus commentaries that provide guidance of immediate and practical benefit to the bench and bar. The Sedona Conference conducts a "regular season" of limited-attendance conferences that are mini-sabbaticals for the nation's leading jurists, lawyers, academics, and experts to examine cutting-edge issues of law and policy. The Sedona Conference also conducts continuing legal education programs under The Sedona Conference Institute (TSCI) banner, an annual International Programme on Cross-Border Data Transfers and Data Protection Laws, and webinars on a variety of topics.

Volume 23, Number 1, of the Journal contains three nonpartisan consensus commentaries from The Sedona Conference Working Group on Electronic Document Retention and Production (WG1), two nonpartisan consensus commentaries from Sedona Canada (WG7), and one nonpartisan consensus commentary from the Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6). I hope you find the commentaries to be thought-provoking, and that they stimulate further dialogue and ultimately serve to move the law forward.

For more information about The Sedona Conference and its activities, please visit our website at www.thesedonaconference.org.

Craig Weinlein
Executive Director
The Sedona Conference
July 2022

The Sedona Conference gratefully acknowledges the contributions of its Working Group Series annual sponsors, event sponsors, members, and participants whose volunteer efforts and financial support make participation in The Sedona Conference and its activities a thought-provoking and inspiring experience.

Journal Editorial Board

The Sedona Conference Advisory Board

The Hon. Jerome B. Abrams (ret.), JAMS, Minneapolis, MN

Kevin F. Brady, Esq., Volkswagen Group of America, Herndon, VA

Prof. Stephen Calkins, Esq., Wayne State University Law School, Detroit, MI

Michael V. Ciresi, Esq., Ciresi Conlin LLP, Minneapolis, MN

The Hon. John Facciola (ret.), Washington, DC

The Hon. James L. Gale (ret.), Greensboro, NC

Prof. Steven S. Gensler, University of Oklahoma College of Law, Norman, OK

Prof. George A. Hay, Cornell Law School, Ithaca, NY

Ronald J. Hedges, Esq., Dentons US LLP, New York, NY

Allan Kanner, Esq., Kanner & Whiteley, L.L.C., New Orleans, LA

The Hon. Paul R. Michel (ret.), Alexandria, VA

Dianne M. Nast, Esq., NastLaw LLC, Philadelphia, PA

The Hon. Nan R. Nolan (ret.), Redgrave LLP, Chicago, IL

The Hon. Kathleen McDonald O'Malley (ret.), Irell & Manella LLP, Washington, DC

The Hon. Andrew J. Peck (ret.), DLA Piper, New York, NY

Jonathan M. Redgrave, Esq., Redgrave LLP, Washington, DC

The Hon. James M. Rosenbaum (ret.), JAMS, Minneapolis, MN

Prof. Stephen A. Saltzburg, George Washington Univ. Law School, Washington, DC

The Hon. Shira A. Scheindlin (ret.), Stroock & Stroock & Lavan LLP, New York, NY

Daniel R. Shulman, Esq., Shulman & Buske PLLC, Minneapolis, MN

Dennis R. Suplee, Esq., Schnader Harrison Segal & Lewis LLP, Philadelphia, PA

Prof. Jay Tidmarsh, University of Notre Dame Law School, Notre Dame, IN

The Hon. Tom I. Vanaskie (ret.), Stevens & Lee, Philadelphia, PA

The Hon. Patrick J. Walsh (ret.), Signature Resolution, Los Angeles, CA

The Hon. Ira B. Warshawsky (ret.), Meyer, Suozzi, English & Klein, P.C., Garden City, NY

Judicial Advisory Board

The Hon. Michael M. Baylson, Senior U.S. District Judge, Eastern District of Pennsylvania

The Hon. Laurel Beeler, U.S. Magistrate Judge, Northern District of California

The Hon. Cathy A. Bencivengo, U.S. District Judge, Southern District of California

The Hon. Cathy Bissoon, U.S. District Judge, Western District of Pennsylvania

The Hon. Hildy Bowbeer, U.S. Magistrate Judge, District of Minnesota

The Hon. Ron Clark, Senior U.S. District Judge, Eastern District of Texas

The Hon. Joy Flowers Conti, Senior U.S. District Judge, Western District of Pennsylvania

The Hon. Mitchell D. Dembin, U.S. Magistrate Judge, Southern District of California

The Hon. George C. Hanks, Jr., U.S. District Judge, Southern District of Texas

The Hon. Susan Illston, Senior U.S. District Judge, Northern District of California

The Hon. Kent A. Jordan, U.S. Appellate Judge, Third Circuit

The Hon. Barbara M.G. Lynn, Chief U.S. District Judge, Northern District of Texas

The Hon. Kristen L. Mix, U.S. Magistrate Judge, District of Colorado

The Hon. Katharine H. Parker, U.S. Magistrate Judge, Southern District of New York

The Hon. Anthony E. Porcelli, U.S. Magistrate Judge, Middle District of Florida

The Hon. Xavier Rodriguez, U.S. District Judge, Western District of Texas

The Hon. Lee H. Rosenthal, Chief U.S. District Judge, Southern District of Texas

The Hon. Elizabeth A. Stafford, U.S. Magistrate Judge, Eastern District of Michigan

The Hon. Gail J. Standish, U.S. Magistrate Judge, Central District of California

The Hon. Leda Dunn Wettre, U.S. Magistrate Judge, District of New Jersey

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

THE SEDONA CONFERENCE COMMENTARY ON THE EFFECTIVE USE OF FEDERAL RULE OF EVIDENCE 502(d) ORDERS

A Project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)

Author:

The Sedona Conference

Editors-in-Chief & WG1 Steering Committee Liaisons:

Philip J. Favro — The Hon. Andrew J. Peck (ret.)

Drafting Team Leaders:

Nathaniel C. Giddings — Leeanne Mancari

Drafting Team:

Anthony DiSenso — Howard Goldberg
Todd Heffner — Henry J. Kelston
Daniel Lim — Scott A. Milner
Angelica M. Ornelas — Kaleigh Powell
Jeff Rickard — Cristin K. Traylor

Judicial Observer:

The Hon. Katherine Parker

Staff editor:

David Lumia

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

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, *Commentary on the Effective Use of Federal Rule of Evidence 502(d) Orders*, 23 SEDONA CONF. J. 1 (2022).

PREFACE

Welcome to the final, August 2021, version of The Sedona Conference *Commentary on the Effective Use of Federal Rule of Evidence 502(d) Orders*, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

This *Commentary* is intended to encourage more robust use of Rule 502(d) non-waiver orders. More than 12 years since the adoption of Rule 502 in 2008, there remains an apparent misunderstanding of the differences between Rule 502(d) and Rule 502(b), resulting in the slow adoption of Rule 502(d) orders as a standard in federal litigation. The *Commentary* attempts to clarify the confusion regarding Rule 502(d)'s protections and limitations while also providing guidance in addressing certain challenges with using 502(d) orders.

The *Commentary* was a topic of discussion at the Working Group 1 meetings in 2019 and 2020, and an initial draft was distributed for member comment earlier this year. The draft was revised based on member feedback and subsequently published for public comment. Where appropriate, the comments received during the public comment period have now been incorporated into this final version.

On behalf of The Sedona Conference, I thank all of the drafting team members for their dedication and contributions to this project. Team members who deserve recognition for their work are: Anthony DiSenso, Howard Goldberg, Todd Heffner, Henry Kelston, Daniel Lim, Scott Milner, Angelica Ornelas, Kaleigh

Powell, Jeff Rickard, and Cristin Traylor. The Sedona Conference also thanks Nathaniel Giddings and Leeanne Mancari for serving as the Drafting Team Leaders, and Phil Favro and the Hon. Andrew Peck for serving as Steering Committee Liaisons and Editors-in-Chief. We also wish to recognize the Hon. Katharine Parker for her contributions as Judicial Observer.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; patent remedies and damages; patent litigation best practices; trade secrets; data security and privacy liability; and other "tipping point" issues in the law. 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. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
August 2021

TABLE OF CONTENTS

I. INTRODUCTION

Federal Rule of Evidence ("Rule") 502 governs what happens when there is a "disclosure of communication or information covered by the attorney-client privilege or work-product protection."[1] Congress adopted this Rule in 2008 for two primary reasons. First, it was intended to address the "widespread complaint" that litigation costs related to the protection of privilege have become "prohibitive." Indeed, there was deep concern that an innocent or minor disclosure could result in subject-matter waiver of all privileged communications in a litigation.[2] Second, it was intended to "provide a party with a predictable protection from a court order—predictability that is needed to allow the party to plan in advance to limit the prohibitive costs of privilege and work-product review and retention."[3]

Rule 502 attempts to accomplish these goals primarily through Rule 502(d). Rule 502(d) permits parties to request entry of a court order preventing waiver for privileged documents produced in the proceeding. By so doing, a Rule 502(d) order provides the parties with greater certainty and therefore has greater potential to limit the costs associated with privilege review and retention.

Another important aspect of Rule 502 is that it creates a uniform rubric for assessing the waiver of privilege under Rule

1. FED. R. EVID. 502.

2. FED. R. EVID. 502 Explanatory Note; *see also id*. ("For example, the court order may provide for return of documents without waiver irrespective of the care taken by the disclosing party; the rule contemplates enforcement of 'claw-back' and 'quick peek' arrangements as a way to avoid the excessive costs of pre-production review for privilege and work product."). The Explanatory Note is reproduced in Appendix C.

3. *See* FED. R. EVID. 502(d) Explanatory Note.

502(b). Importantly, Rule 502(b) is the "default" rule; where a Rule 502(d) order is not entered, Rule 502(b) applies.

The Sedona Conference's consistent position is that parties should collectively seek entry of a Rule 502(d) non-waiver order (so-called "Rule 502(d) orders"). As explained in *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*:

> Rule 502(b) establishes a uniform approach in the federal courts to determine whether an inadvertent production results in waiver, and if so, the scope of the waiver. However, *the burden of asserting and proving inadvertence lies with the responding party and that burden can require substantial effort and documentation.* Moreover, given the multiple factors to be considered and the discretion of courts in weighing the factors and the evidence presented, both waiver and its scope remain uncertain. *Parties can reduce the burdens and eliminate many of these uncertainties by asking the court to enter a Rule 502(d) order*.[4]

A lack of understanding, however, regarding Rule 502(d)'s potential benefits and the differences between Rule 502(b) and 502(d) has contributed to a surprisingly slow adoption of Rule 502(d) orders as a standard in federal litigation. Another factor potentially contributing to underuse of Rule 502(d) orders is a

4. The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 150–51 (2018) (emphasis added) [hereinafter *The Sedona Principles, Third Edition*]. Numerous practitioners have also advocated for more widespread embrace of the Rule. *See, e.g.*, John M. Barkett, *Evidence Rule 502: The Solution to the Privilege-Protection Puzzle in the Digital Era*, 81 FORDHAM L. REV. 1589 (2013) (arguing that "lawyers should maximize the use of Rule 502(d) orders").

belief among some practitioners that Rule 502(d) has shortcomings that have reduced its effectiveness.[5]

This *Commentary* addresses these issues to encourage more robust use of Rule 502(d) orders.[6] The *Commentary* is comprised of the following parts:

- Part II provides an overview of Rule 502(b) and Rule 502(d).

---

5. *See* Swift Spindrift, Ltd. v. Alvada Ins., Inc., No. 09 Civ. 9342, 2013 WL 3815970, at *4 (S.D.N.Y. July 24, 2013) (noting that "remarkably few lawyers seem to be aware of [Rule 502(d)'s] existence"); Ranger Constr. Indus., Inc. v. Allied World Nat'l Assurance Co., No. 17-cv-81226, 2019 WL 436555, at *2, n.2 (S.D. Fla. Feb. 4, 2019) (noting that it was "frankly surprised that the sophisticated attorneys in this case did not enter a written [Rule] 502 claw-back agreement early on in this litigation, either separately or as part of an ESI Protocol Agreement" and "encourag[ing] counsel in all cases involving e-discovery to consider the benefits of jointly entering into a [Rule] 502(d) claw-back agreement and/or an ESI Protocol Agreement early on in the case.").

6. The Sedona Conference has addressed various aspects of Rule 502(d) in previous publications and encouraged parties and courts to use this Rule. *See, e.g.*, *The Sedona Principles, Third Edition*, *supra* note 4, at 147–62 ("An effective Rule 502(d) order need not be complex and can simply provide that: (a) the production of privileged or work-product protected documents, including ESI, is not a waiver, whether the production is inadvertent or otherwise, in the particular case or in any other federal or state proceeding, and (b) nothing contained in the order limits a party's right to conduct a review for relevance and the segregation of privileged information and work product material prior to production."); The Sedona Conference, *Commentary on Protection of Privileged ESI*, 17 SEDONA CONF. J. 95, 103–06, 130–40 (2016) ("Principle 2. Parties, counsel, and courts should make use of Federal Rule of Evidence 502(d) and its state analogues"); *see also* Martin R. Lueck & Patrick M. Arenz, *Federal Rule of Evidence 502(d) and Compelled Quick Peek Productions*, 10 SEDONA CONF. J. 229 (2009); Daniel J. Capra, et al., Limitations on Privilege Waiver under New Federal Rule of Evidence 502 (Sedona Conference Voices from the Desert Series CD-ROM, rel. 25, Nov. 2008).

- Part III highlights the benefits of Rule 502(d) orders.
- Part IV outlines the protections and limits of Rule 502(d).
- Part V discusses potential challenges associated with Rule 502(d) orders in certain matters and highlights some considerations for how practitioners and courts could address those issues and still take advantage of the protections Rule 502(d) offers.

Finally, this publication contains three appendices. Appendix A contains "model" language for a proposed Rule 502(d) order (though practitioners should consider additions to this model as necessary). Appendix B contains a list of U.S. district courts that have promulgated model Rule 502(d) orders as of the date of this publication. Appendix C reproduces the Explanatory Note to Federal Rule of Evidence 502.

By both emphasizing how practitioners and jurists may benefit from using Rule 502(d) orders and by noting issues that could otherwise impede their effectiveness, this *Commentary* should result in more widespread use of Rule 502(d) orders.

II. COMPARISON OF RULE 502(b) AND RULE 502(d)

Many practitioners do not fully appreciate the significant differences between Rules 502(b) and 502(d). In order to understand the benefits of using a Rule 502(d) order, it is necessary to understand the default provisions of Rule 502(b) that apply when the parties have not entered a Rule 502(d) order. As a default rule, Rule 502(b) risks leading to waiver of privilege, additional costs of motion practice, and increased burdens on courts. This Part addresses this issue by comparing these subparts.

A. Rule 502(b), Generally

Rule 502(b) is the "default" rule and addresses ***inadvertent*** disclosure.[7] It provides that a disclosure "does not operate as a waiver in a federal or state proceeding" if the responding party shows that three requirements are met:

1. the disclosure was inadvertent;
2. the holder of the privilege or protection took reasonable steps to prevent disclosure; and
3. the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).[8]

Whether a responding party has satisfied the requirements of Rule 502(b) requires a threshold determination of whether the disclosure of the privileged or protected information was inadvertent. As noted in *The Sedona Principles*, this can impose a significant burden on the responding party:

---

7. *See* Great-W. Life & Annuity Ins. Co. v. Am. Econ. Ins. Co., No. 2-11-cv-02082, 2013 WL 5332410, at *14 (D. Nev. Sept. 23, 2013) (noting that Rule 502(b) "applies as a default in the event there is no agreement otherwise.").

8. FED. R. EVID. 502(b).

> [T]he burden of asserting and proving inadvertence lies with the responding party and that burden can require substantial effort and documentation. Moreover, given the multiple factors to be considered and the discretion of courts in weighing the factors and the evidence presented, both waiver and its scope remain uncertain.[9]

As Rule 502(b) further requires, whether a waiver has occurred additionally depends on the court's analysis of the responding party's diligence to prevent the inadvertent disclosure. This can also impose a burden on the courts and the parties, as courts need to evaluate whether a responding party has taken "reasonable steps" to both prevent and rectify the disclosure. In making this determination, the courts generally look to four factors, none of which alone is dispositive:

1. the reasonableness of precautions taken;
2. the time taken to rectify the error;
3. the scope of discovery from which the inadvertent production was made; and
4. the extent of disclosure and the overriding issue of fairness.[10]

These factors are not memorialized in Rule 502(b)'s language because, as the Explanatory Note indicates, Rule 502(b) "is really a set of non-determinative guidelines that vary from case to case. The rule is flexible enough to accommodate any of those

---

9. *See The Sedona Principles, Third Edition*, *supra* note 4, at 150.

10. FED. R. EVID. 502 Explanatory Note (discussing two cases setting forth non-exhaustive factors the courts may assess in the Rule 502(b) inquiry: Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co., 104 F.R.D. 103, 105 (S.D.N.Y. 1985), and Hartford Fire Ins. Co. v. Garvey, 109 F.R.D. 323, 332 (N.D. Cal. 1985)).

listed factors."[11] Thus, courts have considered other factors in addition to those set forth above.[12]

To determine whether a waiver has occurred under Rule 502(b), courts have inquired into the responding party's discovery and review processes to ascertain whether "reasonable steps" were taken to prevent the disclosure of privileged material.[13] For example, if the responding party has used "advanced analytical software applications and linguistic tools in screening for privilege and work product," that tends to support the assertion that the party has taken "'reasonable steps' to prevent inadvertent disclosure."[14] Other pertinent factors may include

11. FED. R. EVID. 502 Explanatory Note.

12. *See, e.g.*, Williams v. District of Columbia, 806 F. Supp. 2d 44, 50 (D.D.C. 2011) (explaining that "how many documents it reviewed relative to its overall production, the complexity of the review required, and the time it had to gather, review, and produce responsive documents" would be relevant factors to consider); *cf.* Thorncreek Apartments III, LLC v. Vill. of Park Forest, No. 08 C 1225, 2011 WL 3489828, at *5 (N.D. Ill. Aug. 9, 2011) (abandoning a multifactor analysis in favor of asking "whether the production was a mistake").

13. Inquiry into the responding party's discovery and review processes as part of the Rule 502(b) analysis is necessary even though "discovery on discovery" is typically disfavored. *See* Gross v. Chapman, No. 19-cv-2743, 2020 WL 4336062, at *2 (N.D. Ill. July 28, 2020) (denying plaintiffs' request for "discovery on discovery" and citing *The Sedona Principles* and related case authority); *see also The Sedona Principles, Third Edition*, *supra* note 4, at 123 ("[A]s a general matter, neither a requesting party nor the court should prescribe or detail the steps that a responding party must take to meet its discovery obligations, and there should be no discovery on discovery, absent an agreement between the parties, or specific, tangible, evidence-based indicia (versus general allegations of deficiencies or mere 'speculation') of a material failure by the responding party to meet its obligations.") (citing cases).

14. FED. R. EVID. 502 Explanatory Note.

the responding party's privilege screening terms, privilege review process, and the number of documents it has produced.[15]

Importantly, Rule 502(b) *does not* require a responding party to review for privilege post-production "to determine whether any protected communication or information has been produced by mistake."[16] However, the rule *does* direct a responding party to address any "obvious indications that a protected communication or information has been produced inadvertently."[17]

Finally, Rule 502(b) also applies to the inadvertent production of privileged or work-product-protected information to a federal office or agency, "including but not limited to an office or agency that is acting in the course of its regulatory, investigative or enforcement authority. The consequences of waiver, and the concomitant costs of pre-production privilege review, can be as great with respect to disclosures to offices and agencies as they are in litigation."[18]

B. Rule 502(d), Generally

Federal Rule of Evidence 502(d) permits either or both parties to request—and the court to enter—an order providing that the attorney-client or work-product protections are not waived in the instant litigation or any other federal or state proceeding

15. *See* Smith v. Auto-Owners Ins. Co., No. 15-cv-1153, 2016 WL 11117291, at *5 (D.N.M. Oct. 5, 2016) (failing to mark document as confidential was indication that defendant did not intend to produce it); Desouza v. Park W. Apartments, Inc., No. 3:15-CV-01668, 2018 WL 625010, at *3 (D. Conn. Jan. 30, 2018) (placing privileged document in public file to which plaintiff had access was not a reasonable precaution).

16. FED. R. EVID. 502 Explanatory Note.

17. *Id*.

18. *Id*.

by the disclosure of privileged or protected documents in that litigation.[19] It provides as follows:

> Controlling Effect of a Court Order: A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other federal or state proceeding.[20]

If a Rule 502(d) order is entered in a litigation, the responding party generally can "claw back" a privileged or protected document it produced simply by notifying the other parties to the litigation that it is doing so. Unless the Rule 502(d) order contains other limitations on clawbacks,[21] the only challenge a requesting party can typically make to this clawback is whether or not the recalled document is, in fact, privileged.[22] Given their ease of use and self-executing relief, Rule 502(d) orders have been often referred to as "get out of jail free cards."[23]

---

19. *See* Cuhaci v. Kouri Grp., LP, No. 20-cv-23950, 2021 WL 767661, at *1 (S.D. Fla. Feb. 26, 2021) ("Federal courts, including those in Florida, routinely enter such [Rule 502(d)] orders upon request of the parties.").

20. FED. R. EVID. 502(d).

21. Other provisions—such as those governing the volume or timing of clawbacks—that parties may choose to include in their Rule 502(d) order are discussed later in this *Commentary*. *See* Part V, *infra*.

22. *See* Brookfield Asset Mgmt., Inc. v. AIG Fin. Prods. Corp., No. 1:09-cv-08285, 2013 WL 142503, at *1 (S.D.N.Y. 2013) (finding that because the court entered a Rule 502(d) order "AIG has the right to claw back privileged meeting minutes, no matter what the circumstances giving rise to their production were").

23. *See* Elizabeth E. McGinn & Tihomir Yankov, *Guarding Against Privilege Waiver In Federal Investigations* (Sept. 20, 2016), *available at* https://buckleyfirm.com/articles/2016-09-20/guarding-against-privilege-waiver-federal-investigations ("It has been well over a year since Judge Andrew Peck gently excoriated the legal community for underusing the not-so-new privilege

Rajala v. McGuire Woods, LLP is instructive on this issue.[24] In *Rajala*, the plaintiff mistakenly produced privileged documents after the court had entered a Rule 502(d) order.[25] The defendant argued that the court should find a waiver, despite the Rule 502(d) order, because the plaintiff allegedly failed to take "reasonable steps" to preserve privilege.[26] The court rejected this argument and instead found that the Rule 502(d) order did not require a showing of "reasonable steps" taken in a pre-production privilege review, and the plaintiff accordingly did not waive privilege regarding these documents.[27] In reaching this conclusion, the court observed with approval the plaintiff's argument that Rule 502(d) was "designed to allow the parties and the Court to defeat the default operation of Rule 502(b) in order to reduce costs and expedite discovery."[28]

---

waiver protections of Federal Rule of Evidence 502(d). He has fondly referred to it as the 'Get Out of Jail Free Card' and offered that 'it is akin to malpractice not to get [a Rule 502(d)] order.'); *see also* Andrew Jay Peck, *A View From the Bench and the Trench(es) in Response to Judge Matthewman's New Paradigm for Ediscovery: It's More Complicated*, 71 FLA. L. REV. F. 143, 149 (2020).

24. Rajala v. McGuire Woods, LLP, No. 08-cv-2638, 2013 WL 50200 (D. Kan. Jan. 3, 2013).

25. *Id.* at *13–14.

26. *Id.* at *3. The defendant's position was that the disclosure of the document amounted to a "document dump" because the plaintiff failed to undertake a pre-production review of the entire DVD that disclosed the privileged communications due to technical difficulties.

27. *Id*.

28. *Id.* at *5. The court continued by observing that the Rule 502(d) order in that case was "designed to reduce the time and costs attendant to document-by-document privilege review, and was entered with the express goal of eliminating disputes regarding inadvertent disclosure of privileged documents, which would disrupt the discovery process and cause the attorneys in this case to expend significant resources and time arguing about what steps were taken to prevent disclosure and to rectify the error." *Id.*

C. *The Interplay Between Rule 502(d) and Federal Rule of Civil Procedure 26(b)(5)(B)*

Federal Rule of Civil Procedure (FRCP) 26(b)(5)(B) sets out the procedures that apply when privileged or work-product information has been disclosed. The rule requires notice by the responding party, upon which the requesting party must, among other things, "promptly return, sequester or destroy the specified information."[29] The provisions of FRCP 26(b)(5)(B) apply whether a clawback is made under Rule 502(d) or Rule 502(b).

FRCP 26(b)(5)(B) does not delineate (beyond the vague term "promptly") deadlines by which a requesting party must act in response to a clawback request. Rule 502(d) and Rule 26(b)(5) permit the parties the flexibility to negotiate such deadlines in a manner best suited to the needs of case.[30]

FRCP 26(b)(5)(B) also allows the requesting party to "promptly present the information" subject to a clawback dispute "to the court under seal for a determination of the [privilege] claim." Some courts hold that presentation of the document sought to be clawed back is necessary for a resolution of the claim.[31] The Advisory Committee Notes to the 2006 amendment to Rule 26 expressly provide: "In presenting the question,

---

29. FED. R. CIV. P. 26(b)(5)(B).

30. Paul W. Grimm, Lisa Yurwit Bergstrom, & Matthew P. Kraeuter, *Federal Rule of Evidence 502: Has It Lived Up to Its Potential?*, 17 J. RICH. J. L. & TECH. 8, 68 (2011) ("Rule 502(d) and (e) and Rule 26(b)(5)(B) are intended to operate in concert to permit parties to negotiate their own non-waiver agreements under whatever terms they want, even if inconsistent with Rule 26(b)(5)(B) or 502(b).").

31. *See* U.S. Home Corp. v. Settlers Crossing, LLC, No. DKC 08-1863, 2012 WL 5193835, at *5 (D. Md. Oct. 18, 2012) ("It would be wholly illogical to read Rule 26(b)(5)(B) as prohibiting the use of documents 'subject to a claim of privilege' when resolving that very claim of privilege.").

the party may use the content of the information only to the extent permitted by the applicable law of privilege, protection for trial-preparation material, and professional responsibility."[32] On the other hand, responding counsel may prefer that the clawed-back documents be returned and the issue before the court decided based on the information in the privilege log.

Given the foregoing, parties may wish to discuss whether any time limits should be included in their Rule 502(d) order (or in a protective order or similar document) or whether (and if so, how) documents or their contents can be submitted to the court as part of a privilege dispute.[33]

32. *See infra* Part IV.K for a discussion of related ethical issues.

33. *See infra* Part V.A for a discussion of the benefits and drawbacks of including specific clawback time limits.

III. THE BENEFITS OF RULE 502(d) ORDERS

The principal advantage of a Rule 502(d) order over Rule 502(b) is the predictability litigants have regarding the protection of privileged information. That predictability can (1) streamline the privilege review process, decreasing costs for the responding party while also reducing the time a requesting party should anticipate receiving and reviewing documents; and (2) promote the conservation of judicial resources.[34] Each of these benefits is discussed below.

A. Streamlining the Privilege Review and Expediting Production

A Rule 502(d) order provides parties with more certainty regarding waiver. Rule 502(d) specifically enables the responding party to develop a privilege review and workflow that best meets the particular needs of the case. For instance, the responding party may tailor the privilege review to the data, costs, and risks at hand without concern that the procedure selected may not be deemed "reasonable" under Rule 502(b). This allows the responding party to avoid a waiver of privilege across all related litigations in the event of an inadvertent disclosure.[35] Another example could involve the responding party assessing whether a more cost-effective privilege review method, like privilege screening, sampling, or even artificial intelligence tools, would better fit the needs of a particular case. This, in

34. The drafters of Rule 502(d) intended these benefits. *See* FED. R. EVID. 502 Explanatory Note.

35. Importantly, attorneys may still have an ethical obligation to take reasonable care to keep privileged information confidential when producing documents and to gain informed consent from the client before disclosing privileged information. *See* Part IV.K, *infra*; *see also* Edwin M. Buffmire, *Enter the Order, Protect the Privilege: Considerations for Courts Entering Protective Orders Under Federal Rule of Evidence 502(d)*, 81 FORDHAM L. REV. 1621 (2013) (citing Model Rule of Professional Conduct 1.6(a)).

turn, has the potential to reduce costs for the responding party.[36] Moreover, such an order might allow a responding party to engage in a truncated privilege review—or none at all—without risking waiver.[37] With a 502(d) order in place, practitioners may feel comfortable that they need not conduct a fail-safe review to avoid potential privilege waiver stemming from inadvertent production.[38] In addition, the responding party will have the option (though not the obligation) to expedite production, which may provide a significant benefit to the requesting party.

B. Conserving Judicial Resources

Rule 502(d) orders also have the potential to reduce motion practice on privilege disputes, thereby conserving judicial resources.[39] This is because the entry of a 502(d) order can allow courts to bypass fact-intensive inquiries regarding a responding party's efforts to satisfy Rule 502(b)'s "reasonable steps" requirements that frequently accompany such motion practice.[40]

---

36. *See* Winfield v. City of New York, No. 15-cv-05236, 2018 WL 2148435, at *4 (S.D.N.Y. May 10, 2018) ("The rule incentivizes parties to voluntarily agree to procedures that will alleviate the burdens of pre-production privilege reviews by offering protection from waiver of privilege to the producing party.").

37. *See Commentary on Protection of Privileged ESI*, *supra* note 6, at 104 (noting that courts can enter Rule 502(d) orders to prevent waivers without regard to the reasonableness of the procedures used to identify privileged documents). Such a practice is best employed through agreement with the requesting party to address burden issues. *See infra* Part IV.I.1.

38. Practitioners should always consider their ethical obligations before agreeing to limit or forgo a privilege review. *See infra* Part IV.K.

39. Rajala v. McGuire Woods, LLP, No. 08-cv-2638, 2013 WL 50200, at *5 (D. Kan. Jan. 3, 2013).

40. *See, e.g.*, Med. Mut. of Ohio v. AbbVie, Inc. (*In re* Testosterone Replacement Therapy Prods. Liab. Litig.), 301 F. Supp. 3d 917, 926 (N.D. Ill. Aug 2018) (accepting the argument that Plaintiff's disclosure was inadvertent and permitting clawback, citing among other reasons, that because the parties

agreed to the 502(d) standard, it is inappropriate to evaluate the time it took to request the clawback because it "conflates the inadvertence inquiry with the question whether, under Rule 502(b)(3), the party took prompt steps to rectify the error."); *see also* Ranger Constr. Indus., Inc. v. Allied World Nat'l Assurance Co., No. 17-cv-81226, 2019 WL 436555, at *2 (S.D. Fla. Feb. 4, 2019) (noting surprise that counsel had not entered into a 502(d) order and lamenting that this has, in part, resulted in the court "expend[ing] extensive judicial resources, including presiding over a two-day evidentiary hearing and oral argument").

IV. USE OF RULE 502(d) ORDERS

The vehicle for obtaining the benefits of Rule 502(d) is through entry of a court order.[41] The simplest form of such an order—already endorsed by The Sedona Conference—tracks the language of Rule 502(d) and can be found in Appendix A.[42] The legislative history of the Rule and litigation concerning the Rule's specific contours, however, have highlighted a number of nuances that practitioners and courts should understand. They are discussed below.

A. Entry of an Order Is Required, but Consent of All Parties Is Not

A court may enter a Rule 502(d) order sua sponte[43] or on motion by a party supported by good cause.[44] Consent of an

41. Parties may enter into such an agreement without entry of a court order pursuant to Federal Rule of Evidence 502(e); however, without entry of a court order pursuant to Rule 502(d), such an agreement is only binding on the parties to the agreement and does not protect the parties from waiver in other cases. *See* FED. R. EVID. 502(e) and Explanatory Note.

42. *See also The Sedona Principles, Third Edition*, *supra* note 4, at 150–51 (noting that Rule 502(d) orders "can simply provide that: (a) the production of privileged or work product protected documents, including ESI, is not a waiver, whether the production is inadvertent or otherwise, in the particular case or in any other federal or state proceeding, and (b) nothing contained in the order limits a party's right to conduct a review for relevance and the segregation of privileged information and work product material prior to production."); *Commentary on Protection of Privileged ESI, supra* note 6, App'x D.

43. *See* Whitaker Chalk Swindle & Sawyer, LLP v. Dart Oil & Gas Corp., No. 4:08-cv-684, 2009 WL 464989, at *4 (N.D. Tex. Feb. 23, 2009) ("[I]t is within this Court's authority to order discovery to proceed and that by complying with such order Dart has not waived the attorney-client or work-product privilege . . . .").

44. *See* Kappel v. Dolese Bros. Co., No. CIV-18-1003, 2019 WL 2411445, at *1 (W.D. Okla. June 7, 2019) (declining to adopt 502(d) provision within proposed Protective Order where moving party had failed to establish good cause for the clawback provision).

adversary is not required.[45] The court in *Rajala v. McGuireWoods, LLP*[46] noted that the following Statement of Congressional Intent Regarding Rule 502(d) makes this clear:

> This subdivision is designed to enable a court to enter an order, *whether on motion of one or more parties or on its own motion*, that will allow the parties to conduct and respond to discovery expeditiously, without the need for exhaustive pre-production privilege reviews, while still preserving each party's right to assert the privilege to preclude use in litigation of information disclosed in such discovery.[47]

The Explanatory Note also points out that the parties' mutual assent is not required for an order to issue.[48] The Sedona Conference reinforced this notion when it declared that "absent good cause shown by one of the parties, courts should enter Rule 502(d) clawback/non-waiver orders as a matter of course when parties fail to appropriately consider and agree upon the entry of such orders."[49] This is an important element, as requesting parties in, e.g., asymmetric lawsuits may not be inclined to agree to a Rule 502(d) order because they will not benefit from its protections. As outlined in Appendix B, *infra*, some courts

---

45. Rajala v. McGuire Woods, LLP, No. 08-cv-2638, 2013 WL 50200, at *3 (D. Kan. Jan. 3, 2013) ("[A] court may fashion an order, upon a party's motion or its own motion, to limit the effect of waiver when a party inadvertently discloses attorney-client privileged information or work product materials.") (footnote omitted).

46. *Id.* at *3.

47. *See* FED. R. EVID. 502(d) Addendum to Explanatory Note, Statement of Congressional Intent (emphasis added).

48. *See* FED. R. EVID. 502 Explanatory Note ("Party agreement should not be a condition of enforceability of a federal court's order.").

49. *Commentary on Protection of Privileged ESI*, *supra* note 6, at 132–33.

include Rule 502(d) order language in their local rules or model orders.

B. Rule 502(d) Orders Do Not Generally Require Language Specifically Overriding Rule 502(b)

Rule 502(d) orders allow parties and courts to circumvent a protracted examination of the Rule 502(b) factors.[50] A minority of courts, however, have held that to avoid analysis of the Rule 502(b) factors, a Rule 502(d) order must explicitly disclaim application of Rule 502(b).[51] This *Commentary* takes the view that an explicit disclaimer of Rule 502(b) is unnecessary because the language of 502(d) stands on its own. Nevertheless, the model 502(d) order in Appendix A to this *Commentary* includes—out of an abundance of caution—a sentence specifically disclaiming application of Rule 502(b).[52]

---

50. *See supra* Part III.B.

51. *See, e.g.*, U.S. Home Corp. v. Settlers Crossing, LLC, No. DKC 08-1863, 2012 WL 3025111, at *2 (D. Md. July 23, 2012) ("To find that a court order or agreement under Rule 502(d) or (e) supplants the default Rule 502(b) test, courts have required that concrete directives be included in the court order or agreement regarding *each* prong of Rule 502(b)") (emphasis original); Luna Gaming-San Diego, LLC v. Dorsey & Whitney, LLP, No. 06cv2804, 2010 WL 275083, at *4 (S.D. Cal. Jan. 13, 2010) (finding that because the protective order governing inadvertent disclosure did "not address under what circumstances failure to object to the use of inadvertently produced privileged documents waives the privilege," Rule 502(b) applied); Absolute Activist Value Master Fund Ltd. v. Devine, 262 F. Supp. 3d 1312, 1322–23 (M.D. Fla. 2017) (finding that when parties refer generally to the protections of Rule 502, courts should apply Rule 502(b)).

52. *See infra* Appendix A at ¶4 ("The provisions of Rule 502(b) do not apply."). This language was not present in the prior versions of model Rule 502(d) orders in the *Commentary on Protection of Privileged ESI*. *See Commentary on Protection of Privileged ESI*, *supra* note 6, Appendices D, E.; *see also* John M. Barkett, *Evidence Rule 502: The Solution to the Privilege-Protection Puzzle in*

C. *Rule 502(d) Orders Should Not Be Limited to "Inadvertent" Disclosures*

Because the text of Rule 502(d) is not limited to "inadvertent" disclosures, Rule 502(d) orders should be drafted in a way that avoids limiting them to inadvertent disclosures.[53] Indeed, by restricting a Rule 502(d) order to inadvertent disclosures, the parties run the risk that the court will engage in a Rule 502(b) analysis to determine whether a disclosure was or was not inadvertent. This is one of the principal problems with 502(b) that 502(d) eliminates.[54] In addition, limiting the order to "inadvertent" disclosures would foreclose the possibility of so-called quick-peek arrangements or production alternatives without a robust privilege review.

---

the Digital Era, 81 FORDHAM L. REV. 1589, 1617 (2013) ("[A] thoroughly drawn Rule 502(d) order should disclaim the application of Rule 502(b).").

53. *Compare* Whitaker Chalk Swindle & Sawyer, LLP v. Dart Oil & Gas Corp., No. 4:08-cv-684, 2009 WL 464989, at *4 (N.D. Tex. Feb. 23, 2009) (rejecting argument that "Rule 502 is limited to inadvertent disclosures"), *with* Abington Emerson Capital, LLC v. Landash Corp., No. 2:17-CV-143, 2019 WL 3521649, at *3 (S.D. Ohio Aug. 2, 2019) (declining to extend a Rule 502(d) order to intentional disclosures).

54. *See, e.g.*, *U.S. Home Corp.*, 2012 WL 3025111, at *6, n.15 (upholding the Magistrate Judge's decision to engage in a Rule 502(b) analysis where the Rule 502(d) order was limited to inadvertently produced documents, noting that this limitation "necessarily contemplated that some degree of precautionary measures be taken by the parties to avoid waiver"); United States v. Sensient Colors, Inc., No. 07-cv-1275, 2009 WL 2905474, at *2, n.4 (D.N.J. Sept. 9, 2009) (engaging a Rule 502(b) analysis where the parties' had stipulated to the following: "The Parties agree that the inadvertent production of privileged documents or information (including ESI) shall not, in and of itself, waive any privilege that would otherwise attach to the document or information produced").

The model Rule 502(d) order set forth in Appendix A contains language—"whether inadvertent or otherwise"—to specifically address this issue.[55]

D. *Rule 502(d) Orders Do Not Cover a Party's Affirmative Use of Its Own Documents*

While Rule 502(d) safeguards a party against *disclosures* of documents (whether inadvertent or not), it does not provide protection when a party *uses* its own documents.[56] This is especially so when the party or its expert uses its own allegedly privileged documents.[57] For instance, in *Bama Companies, Inc. v. Stahlbush Island Farms, Inc.*, a party's expert relied on (and produced) emails that the party later claimed to be privileged.[58] The court found that any privilege had been waived: "Once used in

---

55. *See* Appendix A, ¶¶1, 4, *infra* ("The production of privileged or work-product protected documents, electronically stored information ("ESI") or information, whether inadvertent or otherwise . . . . The provisions of Rule 502(b) do not apply."). The latter language was not present in the prior versions of model Rule 502(d) orders in the *Commentary on Protection of Privileged ESI*. *See Commentary on Protection of Privileged ESI*, *supra* note 6, Appendix D-E.

56. *See, cf.*, Potomac Elec. Power Co. & Subsidiaries v. United States, 107 Fed. Cl. 725, 731 (2012) (noting that Rule 502(d) does not apply to "intentional waivers made in the course of, for example, an advice-of-counsel defense") (*citing* FED. R. EVID. 502(d)); Hostetler v. Dillard, No. 3:13-cv-0351, 2014 WL 6871262, at *4 (S.D. Miss. Dec. 3, 2014) (finding waiver, notwithstanding entry of a Rule 502(d) order where a non-party disclosed allegedly privileged communications in a deposition, and the party claiming privilege did not claim privilege during the deposition).

57. *See* MICHAEL H. GRAHAM, WINNING EVIDENCE ARGUMENTS: ADVANCED EVIDENCE FOR THE TRIAL ATTORNEY § 502:1 (2006) ("The rule is intended to facilitate discovery. It is not intended to permit a party affirmatively to introduce a favorable piece of privileged or protected information while simultaneously protecting unfavorable information.").

58. No. 18-cv-45, 2019 WL 3890922, at *1 (N.D. Okla. Aug. 19, 2019).

this manner by [the party's] testifying expert and produced to opposing counsel, attorney-client privilege was waived, regardless of whether disclosure was inadvertent or intentional."[59] Other cases are in accord.[60] The subject of use of the responding party's document by the requesting party, such as at a deposition, is discussed in Part V.B, *infra.*

E. Rule 502(d) Orders Are Enforceable in Any Federal or State Proceeding

Because Rule 502(d) allows for multijurisdictional protection, Rule 502(d) orders provide assurance to the responding party that disclosure of a privileged document in the federal proceeding that entered the order will not result in a privilege waiver in that litigation or in "any other federal or state proceeding."[61] The Advisory Committee explained that extending

---

59. *Id*. at *2 (citing cases).

60. *See, e.g.*, Wadler v. Bio-Rad Labs., Inc., 212 F. Supp. 3d 829, 853 (N.D. Cal. 2016) ("The Court rejects Bio–Rad's argument that its disclosure of the expert reports does not result in any waiver because they were only offered in support of their Motion to Strike and not to advance their substantive legal positions. The Court finds no authority suggesting that an express and intentional disclosure of privileged communications in litigation does not result in waiver unless it is made in connection with an attempt to prevail on the merits of that party's position rather than simply attempting to gain an advantage on an evidentiary matter.").

61. FED. R. EVID. 502. The Explanatory Note to Rule 502 observes that the drafter's intent behind Rule 502(d)'s multi-jurisdictional protection—namely, that its use as a cost-saving tool would not be as effective if it failed to provide protection outside the particular litigation in which the order was entered. *See* Part III.A, *supra*. For instance, *Whitaker Chalk Swindle & Sawyer, LLP v. Dart Oil & Gas Corp.* upheld this multi-jurisdiction protection when it entered a Rule 502(d) order that protected against waiver of privilege in a related state court proceeding. No. 4:08-cv-684, 2009 WL 464989 (N.D. Tex. Feb 23, 2009). The defendant in *Whitaker Chalk* filed a motion to stay the federal court proceedings due to a concern that producing privileged

the Rule's reach in this manner was intended to result in further cost savings.[62]

F. Rule 502(d) Does Not Govern Previously Disclosed Information or Disclosures Made in State Proceedings

Rule 502(d) is forward-looking. Thus, a document that has been disclosed prior to entry of a 502(d) order (either in the present litigation or in an earlier lawsuit) cannot be clawed back pursuant to Rule 502(d) after the order's entry.[63]

Similarly, Rule 502(d) also does not apply to the disclosure of privileged material in a state proceeding in which there is not a non-waiver order. As the Explanatory Note indicates: "If a disclosure has been made in a state proceeding (and is not the subject of a state-court order on waiver), *then subdivision (d) is*

---

documents in the federal case would result in a waiver of a claim of privilege over those documents in the underlying state court matter. In response, the court issued a Rule 502(d) order and ordered the federal discovery to proceed, stating that there was no reason "why a Texas court would not recognize an order entered under Rule 502." *Id*. at *4.

62. The Explanatory Note observes as follows: "Confidentiality orders are becoming increasingly important in limiting the costs of privilege review and retention, especially in cases involving electronic discovery. But the utility of a confidentiality order in reducing discovery costs is substantially diminished *if it provides no protection outside the particular litigation* in which the order is entered. Parties are unlikely to be able to reduce the costs of pre-production review for privilege and work product *if the consequence of disclosure is that the communications or information could be used by non-parties to the litigation*." FED. R. EVID. 502 Explanatory Note (emphasis added).

63. *See e.g.*, Abington Emerson Capital, LLC v. Landash Corp., No. 2:17-cv-143, 2019 WL 3521649, at *2–4 (S.D. Ohio Aug. 2, 2019) (assessing whether the 502(d) order would be retroactive and deciding it would not apply to documents produced before the time the parties' began negotiating the 502(d) order and reserving judgment on the period the parties were actively negotiating to understand whether documents were produced during that time).

inapplicable. Subdivision (c) would govern the federal court's determination whether the state-court disclosure waived the privilege or protection in the federal proceeding."[64]

G. *Rule 502(d) Applies Only to the Attorney-Client Privilege and Work-Product Protection*

The text of Rule 502 limits its application to the attorney-client privilege and work-product protection,[65] as those terms are defined in Rule 502(g).[66] This being the case, litigants should expect courts to restrict Rule 502(d) orders to these two

64. FED. R. EVID. 502 Explanatory Note.

65. *See* FED. R. EVID. 502 ("The following provisions apply, in the circumstances set out, to disclosure of a communication or information covered by the attorney-client privilege or work-product protection."); *see also* FED. R. EVID. 502 Explanatory Note ("The rule's coverage is limited to attorney-client privilege and work product."); Winfield v. City of New York, No. 15-cv-05236, 2018 WL 2148435, at *4 (S.D.N.Y. May 10, 2018) (Rule 502 "does not address privileges other than attorney-client and work product."); Proxicom Wireless, LLC v. Target Corp., No. 19-cv-01885-Orl-37LRH, Order at 2 (ECF No. 60) (M.D. Fla. Mar. 25, 2020) ("Rule 502 applies to the disclosure of a communication or information covered by the attorney-client privilege or work-product protection.") (internal quotations and citation omitted); Grimm, *supra* note 30, at 3 ("Rule 502 is titled 'Attorney-Client Privilege and Work Product; Limitations on Waiver.' As the title makes clear, the rule applies only to the attorney-client privilege and the work product doctrine. It has no effect on any other evidentiary privilege, such as the vast array of governmental, or other common law privileges, including the confidential marital communications privilege, the psychotherapist-patient privilege, the clergy-communicant privilege, the 'law enforcement' or 'informer's' privilege, and the 'deliberative process' privilege.") (footnotes omitted).

66. Federal Rule of Evidence 502(g) defines "attorney-client privilege" as "the protection that applicable law provides for confidential attorney-client communications" and "work-product protection" is defined as "the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial."

privileges.[67] For example, in *Proxicom Wireless, LLC v. Target Corporation*, the court found that a Rule 502(d) order could not extend to confidential or proprietary information, as those concerns went beyond the plain language of Rule 502(d).[68]

Nevertheless, some courts have extended Rule 502(d) orders to other privileges and protections. For instance, in *Digital Assurance Certification, LLC v. Pendolino*,[69] the court implemented a discovery protocol to govern inspection of forensic images of computer hard drives that purported to extend Rule 502(d)'s protections to "*any other privilege or immunity*."[70] Similarly, in *Hill Phoenix Inc. v. Classic Refrigeration SoCal, Inc.*,[71] a protective order purported to extend Rule 502(d)'s protections to "*any other*

67. The Explanatory Note explains that Rule 502 is limited to attorney-client privilege and work product, and that the Rule was not intended to apply to any other evidentiary privileges. The Note also explains that the definition of work product "materials" is intended to include both tangible and intangible information. FED. R. EVID. 502 Explanatory Note; *but see* Fairholme Funds, Inc. v. United States, 134 Fed. Cl. 680, 686 (2017) (permitting the application of a Rule 502(d) order to the deliberative process and bank examination privileges).

68. Proxicom Wireless, LLC v. Target Corp., No. 6:19-cv-1886, 2020 WL 1671326, at *2 (M.D. Fla. Mar. 25, 2020); *see also* Citizens for Responsibility & Ethics in Washington v. U.S. Dep't of Commerce, No. 18-cv-03022, 2020 WL 4732095, at *2, n.1 (D.D.C. Aug. 14, 2020) ("Some courts have looked to Federal Rule of Evidence 502 for guidance over waiver in the deliberative process privilege context, however, as other judges have noted, the text of Rule 502 is expressly limited to the attorney-client privilege and work-product protection and should not be extended to the deliberative process privilege.") (citations omitted); *The Sedona Principles, Third Edition*, *supra* note 4, at 152 (noting that "parties cannot rely solely upon Rule 502" to protect all their interests in maintaining client confidentiality, other privileged communications, or personal information).

69. No. 6:17-cv-72, 2019 WL 161981, at *6 (M.D. Fla. Jan. 10, 2019).

70. *Id.* (emphasis added).

71. No. 8:19-cv-00695, 2019 WL 3942960, at *7 (C.D. Cal. Aug. 21, 2019).

recognized privilege or protection."[72] Other cases[73] and some model orders contain similar language.[74]

While courts may purport to enter non-waiver orders pursuant to Rule 502(d) affecting privileges beyond the attorney-client privilege and work-product protection, those orders have no stare decisis effect, nor should they be considered persuasive authority for extending the scope of Rule 502(d).[75] This is not to say that a court cannot enter an order that provides coextensive protections for other privileges through the pendency of a litigation. However, it would be relying on its inherent authority to govern the discovery process rather than on Rule 502(d).

---

72. *Id.* at *7 (emphasis added).

73. *See, e.g.*, ANZ Advanced Techs., LLC v. Bush Hog, LLC, No. 09-cv-00228, 2010 WL 11575131, at *11 (S.D. Ala. May 4, 2010) ("Pursuant to Federal Rule of Evidence 502(d), by engaging in the protocol described in this Order, the parties will not waive the attorney-client privilege, work product protection, and/or *any other privilege or immunity* with respect to such disclosure in this case or in any other Federal or State proceeding.") (emphasis added).

74. *See, e.g.*, The Model Stipulated Protective Order for the Western District of Washington, https://www.wawd.uscourts.gov/sites/wawd/files/ModelStipulatedProtectiveOrder.pdf ("[P]ursuant to Fed. R. Evid. 502(d), the production of any documents in this proceeding shall not, for the purposes of this proceeding or any other federal or state proceeding, constitute a waiver by the responding party of any privilege applicable to those documents, including the attorney-client privilege, attorney work-product protection, *or any other privilege or protection recognized by law*.") (emphasis added). In line with this approach, the Seventh Circuit Council on eDiscovery and Digital Information requires parties to discuss "the potential need for a protective order and any procedures to which the parties might agree for handling inadvertent production of privileged information and other privilege waiver issues pursuant to Rule 502(d) or (e) of the Federal Rules of Evidence." *See* https://www.ediscoverycouncil.com/sites/default/files/StandingOrde8_10.pdf.

75. *See* Winfield v. City of New York, No. 15-cv-05236, 2018 WL 2148435, at *5-6 (S.D.N.Y. May 10, 2018) (rejecting precedent entering a nonwaiver order that had no basis in law).

Accordingly, parties could stipulate to protections for other privileges, though that stipulation may not be enforceable in subsequent litigation against non-parties, since they are not protected by the language of Rule 502(d).

H. The Protections of Rule 502(d) Can Be Incorporated into Other Discovery Orders or Protocols

While courts may enter stand-alone 502(d) orders, they may alternatively include provisions addressing Rule 502(d) in ESI[76] protocols or protective orders. Indeed, courts have encouraged the use of Rule 502(d) provisions embedded within model ESI protocols and template protective orders. For example, the template ESI protocol for the Northern District of California incorporates Rule 502(d) language.[77] Appendix B sets out the districts that have such orders by local rule or model orders.

Using district court templates may reduce negotiation time and result in quick entry by the court. In some matters, however, the Rule 502(d) language in a standard model order may only be a starting point for more extensive negotiations.[78] When

---

76. Electronically Stored Information. *See The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition*, 21 SEDONA CONF. J. 263, 303 (2020).

77. *See* United States District Court for the Northern District of California, *E-Discovery (ESI) Guidelines*, https://www.cand.uscourts.gov/forms/e-discovery-esi-guidelines/. Other courts incorporate Rule 502(d) language into their model protective orders. *See, e.g.*, Western District of Washington Model Stipulated Protective Order, https://www.wawd.uscourts.gov/sites/wawd/files/ModelStipulatedProtectiveOrder.pdf ("[P]ursuant to Fed. R. Evid. 502(d), the production of any documents in this proceeding shall not, for the purposes of this proceeding or any other federal or state proceeding, constitute a waiver by the responding party of any privilege applicable to those documents, including the attorney-client privilege, attorney work-product protection, or any other privilege or protection recognized by law.").

78. *See infra* Part V.

including a Rule 502(d) provision within an ESI protocol or protective order, counsel should ascertain whether the order has conflicting language in other provisions that address the treatment of privileged documents or other types of "inadvertent" productions.

I. A "Quick Peek" Arrangement Relying on Rule 502(d) May Only Occur Where Both Parties Consent

A Rule 502(d) order "may provide for the return of documents without waiver irrespective of the care taken by the disclosing party."[79] This being the case, litigants and courts have relied on Rule 502(d) to execute what are known as "quick peek" arrangements.[80] A quick peek occurs when a responding party provides documents to the other side without review for privilege.[81]

---

79. FED. R. EVID. 502 Explanatory Note.

80. *See* Zubulake v. UBS Warburg LLC, 216 F.R.D. 280, 290 (S.D.N.Y. 2003) (explaining that parties may enter into "so-called 'claw-back' agreements that allow the parties to forego privilege review altogether in favor of an agreement to return inadvertently produced privilege documents").

81. *See* Tom Tinkham & Kate Johnson, *eDiscovery Without the Endless Battles What You Need to Know About Electronic Documents to Keep Your Client and Yourself Out of Trouble*, at 18-22, BENCH & BAR OF MINNESOTA, Feb. 2020, at 18 ("One way to limit this cost is the 'quick peek' approach: Parties enter into a clawback agreement coupled with a Rule 502 order, and agree that they will produce all documents, including privileged information, which the producing party can 'claw back' when the privilege nature becomes apparent. . . . The problem with this approach is that once the opponent has seen the privileged communication, they possess and can exploit the information it contains, even though they must return the documents. For this reason, this approach is rarely used.").

1. Agreed Quick Peek

While the Explanatory Note to Rule 502 states that "the rule contemplates enforcement of . . . 'quick peek' arrangements as a way to avoid the excessive costs of pre-production review for privilege and work product,"[82] these arrangements raise potential ethical and strategic pitfalls.[83] Quick peeks are rarely used and can be risky.

First, counsel would be producing documents it has never seen. In addition, commercially sensitive material could be produced. The material produced could include personal data or health information protected under other statutes or laws, thereby risking potential liability for disclosure. The production could contain highly relevant or sensitive material that could harm the responding party's case, of which the responding party should be aware from an advocacy perspective.

Second, once the requesting party has seen privileged documents, their contents cannot be removed from the minds of adversaries even if they do not retain the documents.[84] Accordingly, on the rare occasion when a quick-peek arrangement is contemplated, parties should consider the issue carefully, including setting clear expectations at the outset, obtaining client consent, and considering at least a minimal privilege review including, for example, documents with lawyer names, email

82. FED. R. EVID. 502 Explanatory Note.

83. T*he Sedona Principles, Third Edition*, *supra* note 4, at 124–26, 154–55; Laura C. Daniel, *Note: The Dubious Origins and Dangers of Clawback and Quick-Peek Agreements: An Argument Against Their Codification in the Federal Rules of Civil Procedure*, 47 WM. & MARY L. REV. 663 (Nov. 2005).

84. *See* U.S. Equal Emp't Opportunity Comm'n v. The George Washington Univ., No. 17-cv-1978, 2020 WL 3489478, at *11 (D.D.C. June 26, 2020) (discussing the practical reasons for protecting documents that have not been reviewed for privilege, including that confidentiality of the material will be lost and that the opposing party will know the contents).

addresses, and law firm domains.[85] Notwithstanding these potentially dangerous issues, there are circumstances where litigants have agreed to a quick-peek arrangement, including a lack of resources (time or money) to conduct the review, expediting the exchange of information in advance of settlement discussions when the data is unlikely to have any privileged documents, or instances when a non-party is involved.[86]

2. Compelled Quick Peek

The Sedona Conference has unequivocally stated that "a court may not compel disclosure of privileged attorney-client communications absent waiver or an applicable exception."[87] In fact, courts have recognized that they are forbidden from

85. The Sedona Conference previously stated that, "risks and limitations make 'quick peek' agreements and productions ill-advised for most cases." *The Sedona Principles, Third Edition*, *supra* note 4, at 154–55; *see also id.* at 124–26; Daniel, *supra* note 83.

86. When they are used, quick-peek agreements typically take one of two forms. First, the parties may simply agree that the responding party will produce all documents from one or more sources, with the ability to claw back any documents at a later date if it learns that a document is privileged. Second, the parties may agree to engage in a three-part process, wherein (1) the responding party may make available information without a full review for privilege, but that the responding party reserves the right to later assert privilege protections; (2) the requesting party reviews the documents and selects what it believes should be produced; and (3) the responding party reviews the selected information and withholds any information that the responding party deems privileged. *See* Henry S. Noyes, *Federal Rule of Evidence 502: Stirring the State Law of Privilege and Professional Responsibility with a Federal Stick*, 66 WASH & LEE L. REV. 673, 691-93 (Spring 2009).

87. *See Commentary on Protection of Privileged ESI*, *supra* note 6, at 137 (observing at Comment 2(e) that "a court may enter a Rule 502(d) order *allowing* the parties to engage in a 'quick peek' process, the court cannot *order* a 'quick peek' process over the objection of the producing party. . . . Indeed, due process is implicated when privileged communications are required to be disclosed, even for in camera review.").

compelling disclosure of privileged information.[88] For example, in *U.S. Equal Employment Opportunity Commission (EEOC) v. The George Washington University*, the EEOC argued that the university should be ordered to run searches for privileged names and then produce the documents pursuant to a 502(d) Order.[89] The court correctly recognized that such an order would be an abuse of discretion and would result in privileged materials being produced.[90] The court cited to The Sedona Conference and other case law for the well-established principle that privileged information should be protected and parties should not be compelled to disclose such materials.[91]

Similarly, U.S. Magistrate Judge Katharine Parker refused to compel a quick peek at the request of the plaintiffs in *Winfield v. City of New York*.[92] In doing so, Judge Parker first noted that "[a]s a general matter, Rule 26(b)(1) limits the scope of discoverable information to *nonprivileged* information."[93] In addition to this restriction, the court observed that "the Federal Rules of Evidence do not abrogate common law privileges . . . [or] create an exception to the law of privilege or authorize a court to compel disclosure of privileged information . . ."[94] Citing The Sedona Conference *Commentary on Protection of Privileged ESI*, Judge Parker reasoned that compelled disclosure of privileged

88. *See* Mgmt. Comp. Grp. Lee, Inc. v. Okla. State Univ., No. CIV-11-967, 2011 WL 5326262, at *4, n.6 (W.D. Okla. Nov. 3, 2011) (declining to impose a quick-peek procedure on an unwilling party).

89. *George Washington Univ.*, 2020 WL 3489478, at *3, 9 (D.D.C. June 26, 2020).

90. *Id*. at *11.

91. *Id*. at *10.

92. No. 15-cv-05236, 2018 WL 2148435, at *8 (S.D.N.Y. May 10, 2018).

93. *Id*. at *5 (emphasis in original).

94. *Id*. at *6.

information could also "implicate due process concerns."[95] Judge Parker concluded by unequivocally holding that the Federal Rules of Evidence, the Federal Rules of Civil Procedure, and Second Circuit precedent prohibited the court from authorizing the compelled quick-peek procedure.[96] This is the majority position on the issue.[97]

J. Parties May Be Able to Incorporate Analogous 502(d) Safeguards in Nonfederal Proceedings

Practitioners have tools available to them to incorporate Rule 502(d)-like protections in arbitration, nonjudicial governmental proceedings, and state proceedings.

1. Arbitration and Regulatory Proceedings

Arbitration can require extensive discovery at times, including the production of ESI.[98] The same is true of regulatory

---

95. *Id*. at *6, n.3.

96. *Id*. at *6.

97. *Contra* Fairholme Funds, Inc. v. United States, 134 Fed. Cl. 680, 687–88 (2017) (granting the plaintiff's request for a quick peek of all 1,500 documents withheld by the defendant over the defendant's objection).

98. AMERICAN ARBITRATION ASSOCIATION, COMMERCIAL ARBITRATION RULES AND MEDIATION PROCEDURES (2013), *available at* https://www.adr.org/sites/default/files/Commercial%20Rules.pdf; JAMS Recommended Arbitration Discovery Protocols for Domestic, Commercial Cases, JAMS (Jan. 6, 2010), https://www.jamsadr.com/arbitration-discovery-protocols/. The rules for arbitration permit arbitrators to actively manage discovery that may occur during the arbitration process, including the authority to issue an order safeguarding or limiting the documents exchanged in discovery. *See* COMMERCIAL ARBITRATION RULES AND MEDIATION PROCEDURES, *supra* note 98, at R-23 ("The arbitrator shall have the authority to issue any orders necessary to . . . without limitation: (a) conditioning any exchange or production of confidential documents and information, and the admission of confidential evidence at the hearing, on appropriate orders to preserve such confidentiality").

proceedings, including responding to civil investigative demands and subpoenas issued by federal, state, or local government agencies that are served during the investigative phase before a judicial proceeding.[99] However, there are no automatic protections for the disclosure of privileged materials in arbitrations or nonjudicial governmental proceedings.

The responding party may minimize the risk of waiving privilege by entering into a written agreement (similar to a stipulation under Rule 502(e))[100] with the requesting governmental entity or entities or seek an order from the arbitrator. The agreement or order should prevent disclosure of any produced documents beyond the use of the requesting party, require the return of any disclosed privileged documents, and preclude the use of any clawed-back privileged documents.

This type of agreement would not bind non-parties to the agreement. For example, it would not bind the parties to a

99. *See* 31 U.S.C. § 3733 (2009) (authorizing the Attorney General, or designee, to issue civil investigative demands and request documents or other discovery materials during the investigative phase, prior to a judicial proceeding); NYC Charter 2203 (authorizing the Commissioner of the New York City Department of Consumer Affairs to serve subpoenas in furtherance of investigating consumer protection matters); Sea Salt, LLC v. Bellerose, No. 2:18-CV-00413, 2020 WL 2114922, at *4 (D. Me. May 4, 2020) (granting defendant's motion to compel privileged documents disclosed to the Federal Bureau of Investigation, and stating that, "[b]y disclosing the communications to the FBI, as to the attorney-client privilege, 'there is no doubt that [Plaintiff] waived any privilege it might have claimed as to the document itself.' . . . Disclosure of the information to law enforcement . . . [is] inconsistent with keeping it from the defendants insofar as the information would likely be disclosed as part of any criminal proceeding.") (internal citations omitted).

100. *See* FED. R. EVID. 502(e) ("An agreement on the effect of disclosure in a federal proceeding is binding only on the parties to the agreement, unless it is incorporated into a court order.").

private follow-on action based on the arbitration or government investigation.[101]

2. State Proceedings Without a Parallel to Rule 502(d)

While several states have adopted versions of Rule 502(d), the majority of states do not have a Rule 502(d) equivalent.[102] However, even in states without an equivalent rule of evidence, the parties may decide to execute a non-waiver agreement or employ other state court tools to address the issues.[103]

Where the parties execute a non-waiver agreement, even in states without a Rule 502(d) equivalent, Federal Rule of Evidence 502(c) may provide protection in any subsequent federal litigation. Rule 502(c) provides protection in federal court if the privilege would not have been waived if the document had been produced in a federal proceeding under Rule 502, *or* there would not have been a waiver under the law of the state where the disclosure occurred.[104] Where the privileged status of a document would not have been waived in the underlying state

---

101. *See* Statement of Congressional Intent Regarding Rule 502 of the Federal Rules of Evidence, 154 CONG. REC. H. 7817–19 (2008) (noting that Rule 502 "does not provide a basis for a court to enable parties to agree to a selective waiver of the privilege, such as to a federal agency conducting an investigation"); *see also In re* Pac. Pictures Corp., 679 F.3d 1121, 1129 (9th Cir. 2012) ("The only justification behind enforcing such agreements would be to encourage cooperation with the government. But Congress has declined to adopt even this limited form of selective waiver.") (citing Statement of Congressional Intent Regarding Rule 502 of the Federal Rules of Evidence).

102. *See Commentary on Protection of Privileged ESI*, *supra* note 6, at Appendix F; *see also* N.J. R. EVID. 530(4) (effective July 1, 2020).

103. *See, e.g.*, ARIZ. R. EVID. 502(d); COLO. R. EVID. 502(d); DEL. R. EVID. 510(d, f); ILL. R. EVID. 502(d); IND. R. EVID. 502(d); IOWA. R. EVID. 5.502(d); MD. R. CIV. P. CIR. CT. 2-402(e)(5); N.J. R. EVID. 530(c)(4); VA. CODE § 8.01–420.7(c); VT. R. EVID. 510(b)(4); WASH. R. EVID. 502.

104. FED. R. EVID. 502(c).

court action, the application of Rule 502(c) confers de facto protection in a federal proceeding.[105]

For example, in *United States Fire Insurance Co. v. City of Warren*, the requesting party moved to compel, claiming that the production of attorney-client privileged documents in a state court proceeding served as a waiver in the subsequent federal proceeding.[106] In response, the court held that Rule 502(c) required it to apply the more protective of federal or state (Michigan) law. Because the production would not have served as a waiver under Michigan law, the court denied the motion to compel production of the documents previously produced in state court.[107]

K. Rule 502(d) and Counsel's Ethical Obligations

There are times when a party may decide to produce documents without performing a thorough privilege review. If a 502(d) order has been entered, the responding party should have the benefit of not waiving privilege on those documents. Nevertheless, clients may not be well served by the production

---

105. *See* FED. R. EVID. 502 Explanatory Note ("The rule does not address the enforceability of a state court confidentiality order in a federal proceeding, as that question is covered both by statutory law and principles of federalism and comity.") (citing 28 U.S.C. § 1738 (providing that state judicial proceedings "shall have the same full faith and credit in every court within the United States . . . as they have by law or usage in the courts of such State . . . from which they are taken")).

106. U.S. Fire Ins. Co. v. City of Warren, No. 2:10-cv-13128, 2012 WL 1454008 (E.D. Mich. Apr. 26, 2012).

107. *Id.* at *16–17; *see also* Tucker v. Ohtsu Tire & Rubber Co., 191 F.R.D. 495, 499 (D. Md. 2000) (noting that a federal court considering the enforceability of a state confidentiality order is "constrained by principles of comity, courtesy, and . . . federalism"). Thus, a state court order finding no waiver in connection with a disclosure made in a state court proceeding is enforceable under existing law in subsequent federal proceedings)).

of privileged documents even when balanced against the client's interest in saving time or resources associated with a lengthier privilege review. Before deciding to proceed in this manner, the lawyer for the responding party should consider potential ethical issues.[108]

In addition, counsel should obtain client approval before producing documents without performing a privilege review or performing only a limited review. The pros and cons of the approach should be clearly explained to the client, as once the requesting party has reviewed a privileged document, it would have knowledge of the legal advice and strategy contained therein, even if the requesting party must return the physical document or ESI.[109]

---

108. Rule 1.6 of the American Bar Association (ABA) Model Rules of Professional Conduct imposes an ethical duty for lawyers to maintain their client's confidences and "not reveal information relating to the representation of a client unless the client gives informed consent." MODEL RULES OF PROF'L CONDUCT R. 1.6 (AM. BAR. ASS'N 2019). In addition, "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." *Id*. Further, Model Rule 1.15 involves a lawyer's duty to "ensure the safekeeping of their client's property, which includes their documents and ESI." *Id*., R. 1.15; *see also The Sedona Principles, Third Edition*, *supra* note 4, at 161. Obtaining a Rule 502(d) order can provide additional protection to client confidences. *See* Buffmire, *supra* note 35, at 1628–29. Lawyers may enhance their "zealous representation" and better safeguard a client's confidences by having a Rule 502(d) order in place, so that any produced privileged documents can potentially be returned without waiver implications. *See The Sedona Principles, Third Edition*, *supra* note 4, at 160.

109. *See* Paula Schaefer, *The Future of Inadvertent Disclosure: The Lingering Need to Revise Professional Conduct Rules*, 69 MD. L. REV. 195, 238–39 (2010) ("[C]lient can only provide 'informed' consent if attorneys explain the factual and legal issues relevant" to privilege review protocols that may have a higher risk of inadvertent disclosure); *see also* Buffmire, *supra* note 35, at 1629 (suggesting that "attorneys should counsel clients about the benefits of Rule 502(d), not unilaterally decide to disclose privileged information").

Finally, production of privileged documents may raise ethical issues for the requesting party.[110] Every state has adopted a unique set of mandatory ethics rules, and lawyers should consult the appropriate set of ethics rules in their jurisdiction to determine whether they are permitted to review an inadvertently produced privileged document. Some states do not prohibit review,[111] while others contain a requirement to notify the responding party of the potentially privileged document.[112] Some jurisdictions explicitly require lawyers who receive inadvertently produced privileged information to stop reading the document.[113] The parties could agree to a provision requiring the requesting party to immediately cease review of the document and notify the responding party of the privileged document production even if not mandated by applicable ethical rules.

---

110. *See* Novartis Pharms. Corp. v. Superior Court, No. D077934, 2021 WL 1918774 (Cal. App. Ct. May 13, 2021) (describing the ethical duties of counsel for the requesting party in California upon their discovery of an inadvertently produced privileged document).

111. *See, e.g.*, RULES REGULATING THE FLORIDA BAR, r. 4-4.4(b) (Fla. Bar).

112. ILL. SUP. CT. R. 4.4(b) ("A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows that the document or electronically stored information was inadvertently sent shall promptly notify the sender.").

113. D.C. RULES OF PROF'L CONDUCT, r4.4(b) (D.C. BAR) ("A lawyer who receives a writing relating to the representation of a client and knows, before examining the writing, that it has been inadvertently sent, shall not examine the writing, but shall notify the sending party and abide by the instructions of the sending party regarding the return or destruction of the writing."). A comment to that rule provides more explanation. *See* D.C. RULE 4.4 cmt. [2] ("Consistent with Opinion 256, paragraph (b) requires the receiving lawyer to comply with the sending party's instruction about disposition of the writing in this circumstances [sic], and also prohibits the receiving lawyer from reading or using the material. . . . ABA Model Rule 4.4 requires the receiving lawyer only to notify the sender in order to permit the sender to take protective measures, but Paragraph (b) of the D.C. Rule 4.4 requires the receiving lawyer to do more.").

V. USING RULE 502(d) ORDERS TO PROMOTE CERTAINTY AND CLARITY DURING PRIVILEGE DISPUTES

Despite the potential for faster productions, cost savings, and certainty offered by Rule 502(d) orders, a significant number of lawyers and courts still rely on Rule 502(b).[114] There are myriad reasons for this, including confusion and a general lack of familiarity with Rule 502(d) orders or concern that a simple 502(d) order is not sufficiently detailed and will lead to undesired consequences.[115] This *Commentary* discusses ways below in which parties and the courts can address these issues—not by relying on Rule 502(b), but by entering into a Rule 502(d) order.

The "model" 502(d) order attached to this *Commentary* is likely sufficient in most cases. Where parties wish to address clawback issues in more detail, they can consider additional provisions. As U.S. District Judge Paul Grimm has observed, more specificity may protect against the risk of nonenforcement by the court.[116] As a result, more specificity may result in greater predictability, particularly when the parties have considered the different scenarios that may arise in a case and delineated the process to follow if they arise.

Against this backdrop, the *Commentary* explores various issues where the parties may consider additional specificity for

---

114. For example, not all District Courts have addressed privilege nonwaiver issues in their adopted rules or model orders. *See* Appendix B.

115. For instance, the requesting party might be concerned that a Rule 502(d) order may allow an opponent to perform a "data dump," thereby potentially shifting the burden of a privilege review to the requesting party while shielding the responding party from the consequences of this tactic.

116. Grimm, *supra* note 30, at 78 ("[I]n drafting a nonwaiver agreement, parties should pay particular attention to whether they should impose upon themselves a particular deadline within which they must give the notice contemplated by Federal Rule of Civil Procedure 26(b)(5)(B) that they are invoking a post-production claim of privilege or work-product protection.").

clawback provisions within 502(d) orders. In connection with the discussion of these issues, the *Commentary* examines some of the principal benefits and drawbacks of providing additional specificity in a 502(d) order.

A. Should the Rule 502(d) Order Set Clear Deadlines and Processes for Challenging Clawbacks?

As noted above, neither Rule 502(d) nor Rule 26(b)(5)(B) specify the time period in which a clawback (or a challenge thereto) needs to be made. In some cases, 502(d) orders lacking such specificity have devolved into time-intensive inquiries the Rule was intended to avoid.[117]

To address this issue, parties may wish to include specific time limits in a 502(d) order to give clear guidance on when they must take particular action after a clawback demand is made. For example, in some cases the parties may consider establishing a specific timeline for events such as (i) when the requesting party must sequester or destroy a document after receiving a clawback demand; (ii) when the responding party must provide either a redacted document or privilege log for the document at issue; (iii) when the requesting party must notify the responding party that it intends to challenge the clawback demand; (iv) when the parties must meet and confer regarding the challenge; and (v) the timing of any motion practice. Specific procedures addressing each of these scenarios may save time and expense in the future by giving parties clear direction on what they must do and when they must do it in the event of a dispute.

117. *Id*. at 78 ("[A] number of reviewing courts have held that parties were not entitled to the protection of non-waiver agreements they drafted because they failed to particularize what they were to do, and when they were to do so, upon discovering that privileged or protected information had been disclosed, or they failed to comply with the procedures that had been drafted into the agreement.") (footnote omitted).

Documenting the procedures can further the goal of predictability and provide more certainty as to the status of documents subject to a clawback demand.

This type of provision can create the potential for additional disputes. For example, a provision that establishes a timeframe for challenging a clawback demand could lead to litigation over whether the challenge was timely. These issues should be weighed when deciding whether to include additional clawback provisions beyond a basic 502(d) order.

B. Should the Rule 502(d) Order Distinguish Between Documents that Have Been "Used" and Documents That Have Been "Disclosed"?

Whether the Rule 502(d) order makes a meaningful distinction between "disclosure" and "use" or other similar words is a potentially important one. It could be argued that because Rule 502(d) (and Rule 502(b)) only uses the term "disclosure," the Rule does not provide protection once a document has been "used," such as at a deposition or a hearing.[118]

For example, in a deposition, if a document is shown to the deponent and the defending attorney immediately prevents any questioning about the contents of the document, the document has only been "disclosed," but not "used." In contrast, if the defending attorney fails to prevent such questioning, the

118. As the Eastern District of New York observed, "while an appropriately worded protective order may prevent waiver due to a producing party's disclosure of privileged information, that party's subsequent failure to timely and specifically object to the use of that information—during a deposition, for example—can waive any applicable privilege." Certain Underwriters at Lloyd's, London v. Nat'l R.R. Passenger Corp., 218 F. Supp. 3d 197, 201 (E.D.N.Y. 2016); *cf. Commentary on Protection of Privileged ESI*, *supra* note 6, at 128–29 (discussing the difference between "use" and "disclosure" under Rule 502(d), but with respect to the responding party).

document has been both "disclosed" and "used." A party's ability to claw back a "used" document is arguably thornier than the ability to claw back a "disclosed" document, as courts typically hold that the privilege has been waived if the clawback does not occur shortly after the time the responding party learns of the use.[119] Nevertheless, it may not be immediately apparent at the deposition that the document shown to the witness is privileged. Should the defending party have a reasonable time after the deposition to make that determination? Courts have discretion on a case-by-case basis to consider what constitutes timely action and from when it is measured.[120] The parties may, or may not, wish to include provisions addressing this issue in a basic 502(d) order.

---

119. *See, e.g.*, Entrata, Inc. v. Yardi Sys., Inc., No. 2:15-cv-00102, 2018 WL 5438129, at *2 (D. Utah Oct. 29, 2018) (holding that the responding party was not entitled to claw back a document after it effectively waived any applicable privilege by failing to seek to preclude the introduction and use of the document during a deposition despite a protective order provision preventing waiver due to a party's disclosure of privileged information); Arconic Inc. v. Novelis Inc., No. 17-cv-1434, 2019 WL 911417, at *2 (W.D. Pa. Feb. 26, 2019) (holding that the responding party must raise the privilege in a timely manner once the document is used or otherwise identified).

120. Klein v. Facebook, Inc., No. 20-cv-08570-LHK (VKD), 2021 U.S. Dist. LEXIS 105516, at *21 (N.D. Cal. June 3, 2021) ("the Court appreciates that some claims of privilege may not be identified until after a transcript is prepared. In such circumstances, it is important that the privilege claim be made promptly."); *see also* Novartis Pharms. Corp. v. Superior Court, No. D077934, 2021 WL 1918774 (Cal. App. Ct. May 13, 2021) (finding waiver where defendant objected to plaintiff's use of an inadvertently produced document during deposition but then failed to "promptly request" the return of that document, waiting over five months to do so).

C. *Should the Rule 502(d) Order Set an Outer Limit on the Number of Documents that Can Be Subject to a Clawback?*

Rule 502(d) orders typically do not set a limit on the number of documents subject to a clawback. A common reason for this is the possibility of technical or vendor errors, leading to a production of a large number of privileged documents. The responding party's protection may be severely limited if the 502(d) order sets a restriction on the number of clawbacks. This could affect the waiver analysis of those documents in the instant litigation and any future action.

If a responding party makes a "data dump" without a privilege review, this could unfairly shift the burden of review to the requesting party. If a responding party plans to produce a large number of documents without review, the parties may want to discuss setting a limit on the number of clawbacks. If the purpose of the limited review is to produce documents as quickly as possible pursuant to the demands of the requesting party, then such a limit would be unwarranted. If, however, this limited review is being performed over the objection of the requesting party, methods for handling the issue could include: (1) The parties could determine a set number of documents that can be clawed back; or (2) they could designate a percentage of total documents produced, and the protections of the parties' 502(d) order could expire or revert to the 502(b) default standard for future productions. Such an approach could strike a balance between a responding party's interest in protecting privileged documents and a requesting party's need to prepare the matter for trial without the universe of available evidence continually or dramatically shifting during the course of the

litigation.[121] As an alternative to limits on the number of clawbacks, the parties may consider including a meet-and-confer provision in the 502(d) order to address this or other issues if they arise.

Litigants concerned about voluminous or late clawbacks should attempt to reach agreement on language that could address those concerns while still providing the benefits of Rule 502(d). Nevertheless, counsel should recognize that these provisions can be a double-edged sword, since each party may need to claw back documents subject to these provisions. The parties should carefully consider the direct and collateral impacts of such a provision.

121. Cost allocation could be a way to deal with burdens resulting from excessively voluminous clawbacks, though responding parties may view this as being extreme and balk at its inclusion.

VI. CONCLUSION

The Sedona Conference continues to recommend obtaining a Rule 502(d) order, most often in the form found in Appendix A to this *Commentary*, in every case in federal court.

APPENDIX A: MODEL RULE 502(d) ORDER

[COURT NAME]
[DISTRICT OR COUNTY]

_____ Plaintiff(s),	)	
vs.	)	CASE NO: _____
_____ Defendant(s).	)	

[PROPOSED] RULE 502(d) ORDER

1. The production of privileged or work-product protected documents, electronically stored information ("ESI") or information, whether inadvertent or otherwise, is not a waiver of the privilege or protection from discovery in this case or in any other federal or state proceeding. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d).

2. Nothing contained herein is intended to or shall serve to limit a party's right to conduct a review of documents, ESI

or information (including metadata) for relevance, responsiveness and/or segregation of privileged and/or protected information before production.

3. The provisions of Rule 502(b) do not apply.

SO ORDERED.

Dated: [City], [State]

[DATE]

_____

[Judge Name]

APPENDIX B: MODEL RULE 502(d) ORDERS FROM DISTRICT COURTS

Court	Model / Standing Order?	Other Guidance (Hyperlink)
	Local Rule or Model / Standing Order (Hyperlink)	
Northern District of Alabama	No	
Middle District of Alabama	No	
Southern District of Alabama	No	
District of Alaska	No	
District of Arizona	No	
Eastern District of Arkansas	No	
Western District of Arkansas	No	
Central District of California	No	
Eastern District of California	No	

Court	Model / Standing Order?	Other Guidance (Hyperlink)
	Local Rule or Model / Standing Order (Hyperlink)	
Northern District of California	Yes	[Model] Stipulation & Order Re: Discovery Of Electronically Stored Information for Patent Litigation Guidelines For The Discovery Of Electronically Stored Information
	[Model] Stipulated Order Re: Discovery Of Electronically Stored Information For Standard Litigation	
Southern District of California	Yes	
	Model Protective Order (Patent Cases) [At 97]	
District of Colorado	No	Guidelines Addressing The Discovery Of Electronically Stored Information
District of Connecticut	No	
District of Delaware	No	Default Standard For Discovery, Including Discovery of Electronically Stored Information

Court	Model / Standing Order?	Other Guidance (Hyperlink)
	Local Rule or Model / Standing Order (Hyperlink)	
District of Columbia	No	
Northern District of Florida	No	
Middle District of Florida	No	Middle District Discovery handbook
Southern District of Florida	No	Sedona Conference Model Rule 502(D) Order
Northern District of Georgia	No	
Middle District of Georgia	No	
Southern District of Georgia	No	
District of Guam	No	
District of Hawaii	No	
District of Idaho	No	

Court	Model / Standing Order?	Other Guidance (Hyperlink)
	Local Rule or Model / Standing Order (Hyperlink)	
Northern District of Illinois	No	Protective Orders - Special Provisions
Central District of Illinois	No	
Southern District of Illinois	Yes	Joint Report Of Parties And Proposed Scheduling And Discovery Order (Class Action)
	Joint Report Of Parties And Proposed Scheduling And Discovery Order	
Northern District of Indiana	No	
Southern District of Indiana	No	
Northern District of Iowa	No	
Southern District of Iowa	No	

Court	Model / Standing Order?	Other Guidance (Hyperlink)
	Local Rule or Model / Standing Order (Hyperlink)	
District of Kansas	No	Guidelines For Agreed Protective Orders For The District Of Kansas Guidelines For Cases Involving Electronically Stored Information
Eastern District of Kentucky	No	
Western District of Kentucky	No	
Eastern District of Louisiana	No	Guidelines For The Discovery Of Electronically Stored Information
Middle District of Louisiana	No	
Western District of Louisiana	No	
District of Maine	No	

Court	Model / Standing Order?	Other Guidance (Hyperlink)
	Local Rule or Model / Standing Order (Hyperlink)	
District of Maryland	No	Principles For The Discovery Of Electronically Stored Information In Civil Cases Discovery Guidelines For The District Of Maryland [at 118]
District of Massachusetts	No	
Eastern District of Michigan	No	Model Order Relating To The Discovery Of Electronically Stored Information Model Case Management And Scheduling Order For Patent Cases
Western District of Michigan	No	
District of Minnesota	No	

Court	Model / Standing Order?	Other Guidance (Hyperlink)
	Local Rule or Model / Standing Order (Hyperlink)	
Northern District of Mississippi	No	Local Uniform Civil Rules
Southern District of Mississippi	No	Local Uniform Civil Rules
Eastern District of Missouri	No	
Western District of Missouri	Yes	Principles For The Discovery Of Electronically Stored Information
	Rule 502(D) Model Order	
District of Montana	No	
District of Nebraska	No	Rule 502 Of The Federal Rules Of Evidence
District of Nevada	No	
District of New Hampshire	No	
District of New Jersey	No	

Court	Model / Standing Order?	Other Guidance (Hyperlink)
	Local Rule or Model / Standing Order (Hyperlink)	
District of New Mexico	No	
Eastern District of New York	No	
Northern District of New York	Yes	
	Confidentiality Order (Patent)	
Southern District of New York	No	
Western District of New York	Yes	
	Local Patent Rules	
Eastern District of North Carolina	Yes	
	Default Protective Order In A Patent Case	
Middle District of North Carolina	No	
Western District of North Carolina	No	

Court	Model / Standing Order?	Other Guidance (Hyperlink)
	Local Rule or Model / Standing Order (Hyperlink)	
District of North Dakota	No	
District of the N. Mariana Islands	No	
Northern District of Ohio	No	
Southern District of Ohio	Yes	Two-Tier Protective Order
	One-Tier Protective Order	
Eastern District of Oklahoma	No	
Northern District of Oklahoma	No	
Western District of Oklahoma	No	
District of Oregon	Yes	
	Model Order Regarding E-Discovery In Patent Cases	

Court	Model / Standing Order?	Other Guidance (Hyperlink)
	Local Rule or Model / Standing Order (Hyperlink)	
Eastern District of Pennsylvania	No	
Middle District of Pennsylvania	No	
Western District of Pennsylvania	Yes	Appendix LCvR 16.1.A [at 10]
	Local Rules Of Court	
District of Puerto Rico	No	
District of Rhode Island	No	
District of South Carolina	No	
District of South Dakota	No	
Eastern District of Tennessee	No	
Middle District of Tennessee	No	
Western District of Tennessee	Yes	
	Stipulated Patent Case Protective Order	

Court	Model / Standing Order?	Other Guidance (Hyperlink)
	Local Rule or Model / Standing Order (Hyperlink)	
Eastern District of Texas	Yes	
	[Model] Order Regarding E-Discovery In Patent Cases	
Northern District of Texas	No	
Southern District of Texas	No	
Western District of Texas	Yes	
	Confidentiality and Protective Order	
District of Utah	No	
District of Vermont	No	Stipulated Discovery Schedule/Order
District of the Virgin Islands	No	
Eastern District of Virginia	No	
Western District of Virginia	No	

Court	Model / Standing Order?	Other Guidance (Hyperlink)
	Local Rule or Model / Standing Order (Hyperlink)	
Eastern District of Washington	No	
Western District of Washington	Yes	
	[Model] Agreement Regarding Discovery of Electronically Stored Information and [Proposed] Order	
Northern District of West Virginia	No	
Southern District of West Virginia	Yes	
	Agreed Order Governing The Inadvertent Disclosure Of Documents Or Other Material Under Rule 502(D)	
Eastern District of Wisconsin	No	
Western District of Wisconsin	No	

Court	Model / Standing Order? Local Rule or Model / Standing Order (Hyperlink)	Other Guidance (Hyperlink)
District of Wyoming	No	

APPENDIX C: EXPLANATORY NOTE ON EVIDENCE RULE 502

The following explanatory note was prepared by the Judicial Conference Advisory Committee on Evidence Rules, revised Nov. 28, 2007:

This new rule has two major purposes:

1) It resolves some longstanding disputes in the courts about the effect of certain disclosures of communications or information protected by the attorney-client privilege or as work product—specifically those disputes involving inadvertent disclosure and subject matter waiver.

2) It responds to the widespread complaint that litigation costs necessary to protect against waiver of attorney-client privilege or work product have become prohibitive due to the concern that any disclosure (however innocent or minimal) will operate as a subject matter waiver of all protected communications or information. This concern is especially troubling in cases involving electronic discovery. *See, e.g., Hopson v. City of Baltimore*, 232 F.R.D. 228, 244 (D. Md. 2005) (electronic discovery may encompass "millions of documents" and to insist upon "record-by-record pre-production privilege review, on pain of subject matter waiver, would impose upon parties costs of production that bear no proportionality to what is at stake in the litigation").

The rule seeks to provide a predictable, uniform set of standards under which parties can determine the consequences of a disclosure of a communication or information covered by the attorney-client privilege or work-product protection. Parties to litigation need to know, for example, that if they exchange privileged information pursuant to a confidentiality order, the court's order will be enforceable. Moreover, if a federal court's confidentiality order is not enforceable in a state court, then the burdensome costs of privilege review and retention are unlikely to be reduced.

The rule makes no attempt to alter federal or state law on whether a communication or information is protected under the attorney-client privilege or work-product immunity as an initial matter. Moreover, while establishing some exceptions to waiver, the rule does not purport to supplant applicable waiver doctrine generally.

The rule governs only certain waivers by disclosure. Other common-law waiver doctrines may result in a finding of waiver even where there is no disclosure of privileged information or work product. *See, e.g., Nguyen v. Excel Corp.*, 197 F.3d 200 (5th Cir. 1999) (reliance on an advice of counsel defense waives the privilege with respect to attorney-client communications pertinent to that defense); *Byers v. Burleson*, 100 F.R.D. 436 (D.D.C. 1983) (allegation of lawyer malpractice constituted a waiver of confidential communications under the circumstances). The rule is not intended to displace or modify federal common law concerning waiver of privilege or work product where no disclosure has been made.

Subdivision (a). The rule provides that a voluntary disclosure in a federal proceeding or to a federal office or agency, if a waiver, generally results in a waiver only of the communication or information disclosed; a subject matter waiver (of either privilege or work product) is reserved for those unusual situations in which fairness requires a further disclosure of related, protected information, in order to prevent a selective and misleading presentation of evidence to the disadvantage of the adversary. *See, e.g., In re United Mine Workers of America Employee Benefit Plans Litig.*, 159 F.R.D. 307, 312 (D.D.C. 1994) (waiver of work product limited to materials actually disclosed, because the party did not deliberately disclose documents in an attempt to gain a tactical advantage). Thus, subject matter waiver is limited to situations in which a party intentionally puts protected information into the litigation in a selective, misleading and unfair manner. It follows that an inadvertent disclosure of

protected information can never result in a subject matter waiver. See Rule 502(b). The rule rejects the result in *In re Sealed Case*, 877 F.2d 976 (D.C. Cir. 1989), which held that inadvertent disclosure of documents during discovery automatically constituted a subject matter waiver.

The language concerning subject matter waiver—"ought in fairness"—is taken from Rule 106, because the animating principle is the same. Under both Rules, a party that makes a selective, misleading presentation that is unfair to the adversary opens itself to a more complete and accurate presentation.

To assure protection and predictability, the rule provides that if a disclosure is made at the federal level, the federal rule on subject matter waiver governs subsequent state court determinations on the scope of the waiver by that disclosure.

Subdivision (b). Courts are in conflict over whether an inadvertent disclosure of a communication or information protected as privileged or work product constitutes a waiver. A few courts find that a disclosure must be intentional to be a waiver. Most courts find a waiver only if the disclosing party acted carelessly in disclosing the communication or information and failed to request its return in a timely manner. And a few courts hold that any inadvertent disclosure of a communication or information protected under the attorney-client privilege or as work product constitutes a waiver without regard to the protections taken to avoid such a disclosure. *See generally Hopson v. City of Baltimore*, 232 F.R.D. 228 (D. Md. 2005), for a discussion of this case law.

The rule opts for the middle ground: inadvertent disclosure of protected communications or information in connection with a federal proceeding or to a federal office or agency does not constitute a waiver if the holder took reasonable steps to prevent disclosure and also promptly took reasonable steps to rectify the error. This position is in accord with the majority view on whether inadvertent disclosure is a waiver.

Cases such as *Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co.*, 104 F.R.D. 103, 105 (S.D.N.Y. 1985) and *Hartford Fire Ins. Co. v. Garvey*, 109 F.R.D. 323, 332 (N.D. Cal. 1985), set out a multi-factor test for determining whether inadvertent disclosure is a waiver. The stated factors (none of which is dispositive) are the reasonableness of precautions taken, the time taken to rectify the error, the scope of discovery, the extent of disclosure and the overriding issue of fairness. The rule does not explicitly codify that test, because it is really a set of non-determinative guidelines that vary from case to case. The rule is flexible enough to accommodate any of those listed factors. Other considerations bearing on the reasonableness of a responding party's efforts include the number of documents to be reviewed and the time constraints for production. Depending on the circumstances, a party that uses advanced analytical software applications and linguistic tools in screening for privilege and work product may be found to have taken "reasonable steps" to prevent inadvertent disclosure. The implementation of an efficient system of records management before litigation may also be relevant.

The rule does not require the responding party to engage in a post-production review to determine whether any protected communication or information has been produced by mistake. But the rule does require the responding party to follow up on any obvious indications that a protected communication or information has been produced inadvertently.

The rule applies to inadvertent disclosures made to a federal office or agency, including but not limited to an office or agency that is acting in the course of its regulatory, investigative or enforcement authority. The consequences of waiver, and the concomitant costs of pre-production privilege review, can be as great with respect to disclosures to offices and agencies as they are in litigation.

Subdivision (c). Difficult questions can arise when 1) a disclosure of a communication or information protected by the attorney-client privilege or as work product is made in a state proceeding, 2) the communication or information is offered in a subsequent federal proceeding on the ground that the disclosure waived the privilege or protection, and 3) the state and federal laws are in conflict on the question of waiver. The Committee determined that the proper solution for the federal court is to apply the law that is most protective of privilege and work product. If the state law is more protective (such as where the state law is that an inadvertent disclosure can never be a waiver), the holder of the privilege or protection may well have relied on that law when making the disclosure in the state proceeding. Moreover, applying a more restrictive federal law of waiver could impair the state objective of preserving the privilege or work-product protection for disclosures made in state proceedings. On the other hand, if the federal law is more protective, applying the state law of waiver to determine admissibility in federal court is likely to undermine the federal objective of limiting the costs of production.

The rule does not address the enforceability of a state court confidentiality order in a federal proceeding, as that question is covered both by statutory law and principles of federalism and comity. *See* 28 U.S.C. § 1738 (providing that state judicial proceedings "shall have the same full faith and credit in every court within the United States . . . as they have by law or usage in the courts of such State . . . from which they are taken"). *See also Tucker v. Ohtsu Tire & Rubber Co.*, 191 F.R.D. 495, 499 (D. Md. 2000) (noting that a federal court considering the enforceability of a state confidentiality order is "constrained by principles of comity, courtesy, and . . . federalism"). Thus, a state court order finding no waiver in connection with a disclosure made in a state court proceeding is enforceable under existing law in subsequent federal proceedings.

Subdivision (d). Confidentiality orders are becoming increasingly important in limiting the costs of privilege review and retention, especially in cases involving electronic discovery. But the utility of a confidentiality order in reducing discovery costs is substantially diminished if it provides no protection outside the particular litigation in which the order is entered. Parties are unlikely to be able to reduce the costs of pre-production review for privilege and work product if the consequence of disclosure is that the communications or information could be used by non-parties to the litigation.

There is some dispute on whether a confidentiality order entered in one case is enforceable in other proceedings. *See generally Hopson v. City of Baltimore*, 232 F.R.D. 228 (D. Md. 2005), for a discussion of this case law. The rule provides that when a confidentiality order governing the consequences of disclosure in that case is entered in a federal proceeding, its terms are enforceable against non-parties in any federal or state proceeding. For example, the court order may provide for return of documents without waiver irrespective of the care taken by the disclosing party; the rule contemplates enforcement of "claw-back" and "quick peek" arrangements as a way to avoid the excessive costs of pre-production review for privilege and work product. *See Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280, 290 (S.D.N.Y. 2003) (noting that parties may enter into "so-called 'claw-back' agreements that allow the parties to forego privilege review altogether in favor of an agreement to return inadvertently produced privileged documents"). The rule provides a party with a predictable protection from a court order—predictability that is needed to allow the party to plan in advance to limit the prohibitive costs of privilege and work product review and retention.

Under the rule, a confidentiality order is enforceable whether or not it memorializes an agreement among the parties

to the litigation. Party agreement should not be a condition of enforceability of a federal court's order.

Under subdivision (d), a federal court may order that disclosure of privileged or protected information "in connection with" a federal proceeding does not result in waiver. But subdivision (d) does not allow the federal court to enter an order determining the waiver effects of a separate disclosure of the same information in other proceedings, state or federal. If a disclosure has been made in a state proceeding (and is not the subject of a state-court order on waiver), then subdivision (d) is inapplicable. Subdivision (c) would govern the federal court's determination whether the state-court disclosure waived the privilege or protection in the federal proceeding.

Subdivision (e). Subdivision (e) codifies the well-established proposition that parties can enter an agreement to limit the effect of waiver by disclosure between or among them. Of course such an agreement can bind only the parties to the agreement. The rule makes clear that if parties want protection against nonparties from a finding of waiver by disclosure, the agreement must be made part of a court order.

Subdivision (f). The protections against waiver provided by Rule 502 must be applicable when protected communications or information disclosed in federal proceedings are subsequently offered in state proceedings. Otherwise the holders of protected communications and information, and their lawyers, could not rely on the protections provided by the Rule, and the goal of limiting costs in discovery would be substantially undermined. Rule 502(f) is intended to resolve any potential tension between the provisions of Rule 502 that apply to state proceedings and the possible limitations on the applicability of the Federal Rules of Evidence otherwise provided by Rules 101 and 1101.

The rule is intended to apply in all federal court proceedings, including court-annexed and court-ordered arbitrations,

without regard to any possible limitations of Rules 101 and 1101. This provision is not intended to raise an inference about the applicability of any other rule of evidence in arbitration proceedings more generally.

The costs of discovery can be equally high for state and federal causes of action, and the rule seeks to limit those costs in all federal proceedings, regardless of whether the claim arises under state or federal law. Accordingly, the rule applies to state law causes of action brought in federal court.

Subdivision (g). The rule's coverage is limited to attorney-client privilege and work product. The operation of waiver by disclosure, as applied to other evidentiary privileges, remains a question of federal common law. Nor does the rule purport to apply to the Fifth Amendment privilege against compelled self-incrimination.

The definition of work product "materials" is intended to include both tangible and intangible information. *See In re Cendant Corp. Sec. Litig.*, 343 F.3d 658, 662 (3d Cir. 2003) ("work product protection extends to both tangible and intangible work product").

[During the legislative process by which Congress enacted legislation adopting Rule 502 (Pub. L. 110–322, Sept. 19, 2008, 122 Stat. 3537), the Judicial Conference agreed to augment its note to the new rule with an addendum that contained a "Statement of Congressional Intent Regarding Rule 502 of the Federal Rules of Evidence." The Congressional statement can be found on pages H7818–H7819 of the Congressional Record, vol. 154 (September 8, 2008).]

The SEDONA CANADA COMMENTARY ON DISCOVERY OF SOCIAL MEDIA

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

Author:

The Sedona Conference

Editors-in-Chief and Drafting Team Leaders:

Matthew Maslow Christopher Walker

Drafting Team:

Lisa Alleyne Gretel Best
Pamela Drummond William Ellwood
Melissa Feriozo Lauren Grimaldi
Kevin Lo David Outerbridge
Molly Reynolds Chuck Rothman
Nic Wall William Walters

Judicial Participants:

Master Kaufman Justice Calum MacLeod

Staff editor:

David Lumia

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

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, Sedona Canada Commentary on Discovery of Social Media, 23 SEDONA CONF. J. 73 (2022).

PREFACE

Welcome to the final, September 2021, version of *The Sedona Canada Commentary on Discovery of Social Media ("Commentary"),* a project of the Sedona Canada Working Group (WG7) of The Sedona Conference. This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and pri-vacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way through the creation and publication of nonpartisan, consensus commentaries and through advanced legal education for the bench and bar.

This *Commentary* was first published for public comment in June 2021. Where appropriate, the comments received during the public-comment period have been incorporated in this final version.

The *Commentary* builds on similar principles and guidelines regarding social media developed by the Sedona Conference Working Group 1 for the United States, including *The Sedona Conference Primer on Social Media,* first published in 2017 and up-dated in 2019. However, this *Commentary* focuses on the regula-tory and practice requirements of the Canadian legal profession.

The Sedona Conference acknowledges the efforts of Editors-in-Chief Matthew Maslow and Christopher Walker, who were invaluable in driving this project forward. We also thank draft-ing team members Lisa Alleyne, Gretel Best, Pamela Drum-mond, William Ellwood, Melissa Feriozzo, Lauren Grimaldi, Kevin Lo, David Outerbridge, Molly Reynolds, Chuck Roth-man, Nic Wall, and William Walters and judicial participants Master Kaufman and Justice Calum MacLeod for their dedica-tion and contributions to this project.

We hope our efforts will be of immediate and practical assistance to legal service providers, related third-party service providers, and their clients. 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
September 2021

TABLE OF CONTENTS

I. THE PERSISTENCE OF SOCIAL MEDIA

Social media is ubiquitous throughout most of the world, with users numbering in the billions irrespective of age, geography, or socioeconomic status. Not only consumers, but also governments and businesses employ social media to communicate with their constituencies and target audiences. With so many individuals and organizations communicating through social media, it is increasingly becoming a subject of discovery in legal proceedings and investigations. Lawyers must understand the different types of social media and the unique discovery issues they present so they can advise and assist their clients in properly preserving, collecting, producing, and requesting such information in discovery.

Specifically, 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.[1] 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.[2] 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.[3]

---

1. See *Toth v City of Niagara Falls*, 2017 ONSC 5670 (CanLII), 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).

2. See *Leduc v. Roman*, 2009 CanLII 6838 (ON SC) [*Leduc*]; *Frangione v. Vandongen*, 2010 ONSC 2823 (CanLII) [*Frangione*]; *Murphy v. Perger*, [2007] OJ No 5511 (WL Can) [*Murphy*], *McDonnell v. Levie*, 2011 ONSC 7151 (CanLII) [*McDonnell*], and *Casco v. Greenhalgh*, 2014 CarswellOnt 2543 (Master) [*Casco*]; *Papamichalopoulos v Greenwood*, 2018 ONSC 2743 and *Wilder v Munro*, 2015 BCSC 183.

3. *Schuster v Royal & Sun Alliance Insurance Company of Canada*, [2009] OJ No 4518 (WL) (ON SC), and see *Stewart v. Kemptster*, 2012 ONSC 7236

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.[4] The plaintiff's computer was used by all members of his family. To protect the privacy rights of non-party family members, the Ontario Court ordered the parties to agree on the use of an independent expert to review the hard drive.

In *Fric v. Gershman*,[5] the Supreme Court of British Columbia similarly sought to protect the privacy of third parties when it ordered production of certain photographs posted on the plaintiff's Facebook page. The plaintiff was permitted to edit the photographs prior to disclosure to protect the privacy of other individuals who appeared in them. The Court in *Fric* refused to order production of commentary from the Facebook site, however, holding that if such commentary existed, the probative value of the information was outweighed by the competing interest of protecting the private thoughts of the plaintiff and third parties.[6] 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.[7]

Even where individuals seek to operate under the privacy that may be afforded by the anonymity of social media profiles,

---

(CanLII), *Garacci v. Ross*, 2013 ONSC 5627 (CanLII), and *Conrod v. Caverley*, 2014 NSSC 35 (CanLII).

4. 2009 BCSC 358 (CanLII), leave to appeal for further production dismissed, 2009 BCCA 555 (CanLII).

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

6. *Ibid* at para 75, citing Dosanjh v. Leblanc and St. Paul's Hospital, 2011 BCSC 1660.

7. *Jones v IF Propco*, 2018 ONSC 23.

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*,[8] 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 because they are critical of public figures. 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.

Section II of the *Sedona Canada Commentary on Discovery of Social Media* discusses traditional and emerging social media technologies and the discovery challenges they present. Section III examines relevance and proportionality in the context of social media. It also explores preservation challenges, collection, and search obligations, together with review and production considerations. Section IV describes the impact of cross-border issues on social media discovery, and Section V explores authentication issues. The *Commentary* concludes in Section VI by analyzing ethical issues that lawyers should consider in connection with social media discovery.

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

II. SOCIAL MEDIA AND EMERGING TECHNOLOGIES

Social media is a broad term that defies precise definition. Social media ranges from traditional platforms and messaging applications to collaboration tools and applications that stream live video. Formats include a combination of text (messages, status updates, comments, blog posts, etc.), photos, graphics, memes (photos with overlay text), infographics, maps (geographic location information), emojis, audio, video, or links to other content. While social media content varies from one platform and application to the next, several consistent concepts continue to emerge: content is shared, interactive, internet-based, professional, or personal. Perhaps most significant for discovery, such content is typically dynamic, it may be easily modified or destroyed by the user, the recipient, the application provider, or by the technology itself.

As social media has expanded into many different areas, a precise definition has become more elusive, particularly since conceptions of what it is have been blurred. Numerous social and professional networking, collaboration, and communication applications may be considered social media. The Oxford English Dictionary defines "social media" as "websites and applications used for social networking." "Social network," in turn, is defined as "the use of dedicated websites and applications to communicate with each other by posting information, comments, messages, images, *etc*."[9] A common characteristic of all social media is the sharing of information—either personal information or, increasingly, work-related information—in either a targeted or broad fashion. Many social media applications have their own direct and group messaging functions, and many instant messaging applications have added features that are common to more traditional forms of social media.

9. Concise Oxford English Dictionary, 12th ed., sub verbo "social media."

Given the variety and fluidity of forms and formats, the *Sedona Canada Commentary on Discovery of Social Media* focuses on the different kinds of social media that exist today, together with their respective discovery challenges. This includes a review of platforms and other traditional forms of social media, various types of messaging applications, live-streaming video applications, location-based social intelligence platforms, and devices using social media applications.[10]

A. Platforms and Other Traditional Forms of Social Media

Discovery of social networking content has generally focused on more traditional platforms, mainly because platform-based social media was the first type of online social networking to be widely embraced and widely used by consumers and organizations.

Although traditional platforms differ from one site to the next, these platforms share many similar features. They allow users to post content to bulletin board-type locations. Privacy settings, when enabled, permit users some control over the initial distribution of their content.[11] Platforms also permit users to exchange messages directly with other users, known as "direct messaging." Direct messaging capability reflects responsiveness to consumer demand for a feature of traditional messaging applications.

Popular social media platforms include Facebook (a social networking site) and Twitter (an electronic bulletin board, social networking, and online news service). Other platforms include

10. Social media data analytics platforms and content distribution portals for posting on social media sites are outside the scope of the *Commentary on Discovery of Social Media in Canada*.

11. See *Frangione v. Vandongen*, 2010 ONSC 2823 (Ont. Sup. Ct. J.) (discussing the impact of privacy settings restricting access to social media on a production order).

LinkedIn (a professional networking site), Instagram (mobile, desktop, and internet-based photo-sharing application and service), Flickr (a photo-sharing site), and YouTube (a site for posting and commenting on video footage). Many of these platforms were initially developed as consumer-based applications funded by advertising. Increasingly, however, businesses, governments, and political campaigns and organizations use these platforms for marketing and communication purposes.

For several years now, requesting parties in litigation have sought to obtain, and responding parties have attempted to preserve and produce, relevant content from social media platforms. Indeed, social media jurisprudence generally reflects discovery of platform-based social media. Some of the more common issues that arise in connection with discovery of platform-based social media include preservation and collection; the nature and scope of a particular request; the role of privacy settings; and issues surrounding possession, custody, and control.[12]

B. Messaging Applications

Reports indicate that users of messaging applications now outnumber users of social media platforms.[13] The advent of more advanced mobile device technology and consumer preference are primarily responsible for this phenomenon.

Relevant information can often be found on a wide variety of messaging applications. Nevertheless, messaging applications are not a homogenous class of data repositories. On the contrary, features such as communication functionality, user

12. See *infra* Section III.

13. See *Messaging Apps Are Now Bigger Than Social Networks* (20 September 2016), online: Bus. Insider Intelligence <http://uk.businessinsider.com/the-messaging-app-report-2015-11?r=US&IR=T>.

information, and content retention vary widely. The following is a brief overview of some of the more common messaging applications and the discovery challenges they may present.

1. Over-The-Top Messaging Applications

Over-the-top (OTT) messaging applications were developed several years ago as an alternative to traditional text messages, i.e., short message service (SMS) messages. Messages sent through OTT applications go directly through the internet from device to device. Unlike text messages, they do not pass through the message servers belonging to SMS providers (telecommunications companies such as Bell or Rogers), private enterprises, or governmental entities.

OTT messaging applications generally offer users enhanced functionality at a lower cost than providers of traditional text messaging services.[14] Such functionality includes, among other things, the ability to send images and video, graphic overlay functionality, and the use of emojis and effects. Certain OTT messaging applications offer end-to-end message encryption. OTT applications generally fall into two categories: third-party applications and operating-system-specific communication systems.[15]

Third-party OTT messaging applications operate across multiple device platforms. This means that users can access application content on smartphones, tablets, laptops, and other devices. In addition, users can download and communicate with

14. See Janet Balis, *What an OTT Future Means for Brands* (13 May 2015), online: Harv. Bus. Rev., online: <https://hbr.org/2015/05/what-an-ott-future-means-for-brands>.

15. See James Chavin, Aadil Ginwala & Max Spear, *The future of mobile messaging: Over-the-top competitors threaten SMS* (Sept. 2012), online: McKinsey & Company <https://www.mckinsey.com/~/media/mckinsey/dotcom/%20client_service/Telecoms/PDFs/Future_mobile_messaging_OTT.ashx>.

these applications on different operating systems (e.g., the Android and the iOS operating systems). Popular third-party OTT applications include WhatsApp, Snapchat, Signal, and Facebook Messenger.

In contrast are operating-system-specific OTT messaging applications such as iMessage—offered exclusively by Apple through its iOS operating system. If an iMessage user sends a message from an iOS device to a device that uses the Android operating system, it is transmitted as a traditional SMS text message rather than as an OTT message. As a result, the enhanced features of iMessage will not be available.

2. Anonymous Chat and Messaging Applications

Anonymous chat and messaging applications allow users to communicate without disclosing their identities. They have grown in popularity due to the perceived freedom that anonymity provides. Anonymous applications such as Blind have been deployed in the workplace to encourage workers to provide candid feedback to their employers without fear of recrimination.[16]

Consumer versions of anonymous messaging applications (such as Whisper and Truth) generally appeal to high school and college students. They are group-oriented; any number of users in a specific geographic area can join in a discussion. Consumer-based applications have gained a certain amount of notoriety due to harassing messages exchanged by application users and other inappropriate conduct.[17]

---

16. See Rosa Trieu, *How Businesses Are Using Anonymous Blind App To Change Work Culture* (2 July 2016), online: Forbes <https://www.forbes.com/sites/rosatrieu/2016/07/02/how-businesses-are-using-anonymous-blind-app-to-change-work-culture/#444d6a9eff81>.

17. See Matt Burns, *After School Is The Latest Anonymous App Resulting In Student Cyberbullying And School Threats* (3 Dec. 2014), online: TechCrunch

3. Ephemeral Messaging Applications

Ephemeral messaging applications enable senders of a message to control its deletion, ranging from immediately upon reading the message (or even after reading each word of the message) to several hours, days, or weeks afterwards.[18] Different applications offer competing features, including the ability to control distribution of messages (to a small group versus a community of users), message encryption, private messaging capability, prevention of screenshots, untraceable messages, and removal of messages from others' devices.[19] Consumer and enterprise-grade versions of these applications, also known as "self-destructing messages" and "disappearing messages," are available from Wickr, Confide, and Snapchat. Other applications such as Facebook Messenger, Signal, and iMessage can be configured to include an ephemeral messaging feature.[20]

<https://techcrunch.com/2014/12/03/after-school-is-the-latest-anonymous-app-resulting-in-student-cyberbullying-and-school-threats/>.

18. See Aarian Marshall, *Uber's Not The Only One That Should Be Wary Of Disappearing Messaging Apps* (17 Dec. 2017), online: Wired <https://www.wired.com/story/uber-waymo-wickr-ephemeral-messaging/>.

19. See generally Agnieszka A. McPeak, "Disappearing Data" (2018) Wis. L. Rev 17 at 32 (discussing various technological features of ephemeral messaging applications).

20. Information from social media which bases communication on timed data (which is deleted after a set period of time) has been mentioned in the Canadian court system. This content itself has been referred to as "disappearing content", or "ephemeral content." Information from these communication mediums can clearly be valuable in court proceedings, and as such, has been requested in the past. In an application for production of documents in the case *Araya v Nevsun Resources Ltd.*, 2019 BCSC 262, personal communications were requested from platforms including Instagram and Snapchat, which use ephemeral content as a central method of communication. However, the production of these documents is another matter in itself. As seen in the court proceedings, information for discovery is limited to that which is within a party's "possession, power and control." The question of whether

4. Cloud-Based Messaging and Collaboration Applications for the Workplace

Cloud-based messaging and collaboration applications are designed to provide users with a more interactive communication platform than traditional enterprise communication tools such as email. Intended for the workplace, these applications have multifaceted functionality, including discussion lines for larger groups, one-on-one messaging exchanges, and confidential messaging channels to share sensitive information.[21] These applications typically maintain communicated content in cloud-based storage, though they may also be deployed on an enterprise's servers. Slack, Asana, HipChat, Jive, Microsoft Yammer, Salesforce Chatter, and VMware's Socialcast are examples of these applications.

5. Discovery Challenges with Messaging Applications

In addition to the discovery issues relating to social media platforms,[22] there are unique issues relating to discovery of relevant messaging application content, such as identifying the origin of anonymous application content. This process often requires unmasking application user identities, which can be a difficult and lengthy process.[23] Unveiling the identity of a message

---

parties must disclose ephemeral content depends on whether such communication is 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 follow.

21. See Philip Favro, Donald Billings, David Horrigan & Adam Kuhn, "The New Information Governance Playbook for Addressing Digital Age Threats" (2017) 3 Rich. J.L. & Tech. Ann. Survey ¶10.

22. See *supra* Section II(A).

23. See *FAQs*, online: Blind <https://www.teamblind.com/faqs> (last visited 28 Dec. 2018) ("[O]ur . . . infrastructure is set up so that user account and activity information is completely disconnected from the email verification process. This effectively means there is no way to trace back your activity on

poster typically hinges on the detail of logs the software provider may maintain on the back end of its application and the duration of time it maintains the logs.

Preserving and collecting relevant messaging application content, particularly from OTT and ephemeral messaging applications, presents an additional challenge. Such content is dynamic. In addition, messaging content is often not backed up or even retained by many application providers and may only be available on the device itself.[24] End-to-end encryption may also prevent access to message content.

C. Live-Streaming Video

Live-streaming video applications are another source that may contain relevant information in discovery. Users of these applications can now share live-streaming content with followers, friends, or others through any number of different applications or platforms, such as Periscope or Facebook Live. Users include organizations that are gravitating toward live video streams because it "is an easy and effective way to interact with people, especially if you use a question and answer style format or another medium that encourages participation."[25]

These considerations also apply to an organization's internal communication tools, such as Zoom, Webex, GoToMeeting, and Microsoft Teams, which can broadcast and record video.

Blind to an email address, because even we can't do it. . . . [Y]our work emails are encrypted and locked away, forever.").

24. See *Vector Transportation Services Inc v. Traffic Tech Inc.*, [2008] OJ No 3500 (Ont. Sup. Ct. J.) (ordering that a computer be inspected by a forensic data recovery expert to retrieve deleted emails).

25. Jason DeMers, "The Top 7 Social Media Trends That Dominated 2016," *Forbes* (7 Dec. 2016), online: <https://www.forbes.com/sites/jaysondemers/2016/12/07/the-top-7-social-media-trends-that-dominated-2016/#7ae6d67c726c>.

Discovery of data from live-streaming video applications involves many of the same issues as those involved in discovery of other social media. These issues include preservation and collection; relevance and proportionality; and power, possession, and control.[26]

D. Location-Based Social Intelligence Platforms

Location-based social intelligence platforms enable searching across social media sites for conversations by keywords and geofencing. Geofencing is a software feature that uses global positioning system or radio frequency identification to define geographical boundaries.[27] To date, law enforcement and news reporters are the most prevalent users. Examples of companies developing and distributing the technology include DigitalStakeout, Echosec, Snaptrends, and Media Sonar.

The technology is still nascent and relies on the social media providers to feed data to these platforms through an application programming interface (API).[28] Mass market adoption of these

---

26. The concept of power, possession, and control is referred to by different terminology in the rules of various Canadian provinces and territories and is also referred to as "possession, custody, and control" in this *Commentary* and other Sedona Conference publications. *See* Section III, *infra*.

27. See Sarah K. White, *What is geofencing? Putting location to work* (Nov. 1, 2017), online: CIO <https://www.cio.com/article/2383123/mobile/geofencing-explained.html>.

28. In March 2017, Facebook updated its policies to prohibit mass surveillance on its platform by explicitly blocking developers from obtaining user data for surveillance purposes. See Elizabeth Dwoskin, "Facebook says police can't use its data for 'surveillance,' " *Wash. Post* (13 March 2017), online: <https://www.washingtonpost.com/news/the-switch/wp/2017/03/13/facebook-says-police-cant-use-its-data-for-surveillance/>. Those policy changes were criticized in 2018 after it was revealed that Cambridge Analytica (and likely other companies) circumvented those policies to mine Facebook users' data. See "The Facebook scandal could change politics as well as the internet:

tools will depend on pricing, availability of data, privacy concerns, and government regulations.

Discovery involving location-based social intelligence platforms will likely focus on issues that are similar to those with other social media. Those issues include preservation and collection; relevance and proportionality; and power, possession, and control.[29]

E. Devices Using Social Media Applications

Devices are not social media platforms in and of themselves. Nevertheless, devices in some instances have been designed to work in conjunction with specific-purpose social media applications. In these circumstances, devices can be considered part of a social media system.

These devices include wearable technologies, which are electronic devices embedded in clothing, jewelry, shoes, or other apparel that transmit or receive data through wireless technology.[30] Users frequently use social media to communicate information found on their wearable technologies.

The data that wearable technologies generate often relates to the users of these technologies. It includes information relating to a user's physical condition and level of exertion (e.g., heart rate, blood pressure, sleep cycles, etc.), together with geolocation information (based on tracking exercise locations for higher-end models).[31] Strava, for instance, is an application that allows users to share publicly or with their authorized followers

---

Even used legitimately, it is a powerful, intrusive political tool," *The Economist* (22 March 2018).

29. See *infra* Section III.

30. See Nicole Chauriye, "Wearable Devices As Admissible Evidence: Technology Is Killing Our Opportunities To Lie" (2014) 24 Cath. U. J. L. & Tech. 495 at 499.

31. *See ibid* at 500–02.

myriad details regarding their running, cycling, and swimming workouts.[32] Because wearable technologies (such as a smart watch) generally are considered temporary storage endpoints and synchronize with mobile and computer devices, they are likely redundant with traditional sources of information found on those technologies.

Additional examples of these devices may be smartphones or game consoles that are connected to the internet where social elements exist.[33] Whether in a smartphone or a stand-alone game console, these devices generate data such as user identities or game results that are designed to be shared over social channels. Examples of games played on these devices include Honor of Kings, Township, and Pokémon Go .

Attempts to discover such data, whether communicated through social media sites or maintained on wearable technology, will encounter issues similar to those posed by platforms and messaging applications. They include preservation and collection; relevance and proportionality; and power, possession, and control.[34]

---

32. See Richard Pérez-Peña & Matthew Rosenberg, "Strava Fitness App Can Reveal Military Sites, Analysts Say," *New York Times* (29 Jan. 2018) online: <https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html>.

33. Social media elements may also be found in social robots such as iPal and in devices that use artificial intelligence. Machine learning, based on human behavior, is used to auto-generate code to better customize the social experience. See Robin Raskin, "Robots on the Runway" (15 June 2016), online: Huff Post <https://www.huffpost.com/entry/robots-on-the-runway_b_10460902>.

34. See *infra* Section III.

III. THRESHOLD DISCOVERY ISSUES

As social media usage becomes more widespread, the challenges of preservation, collection, review, and production of relevant information are receiving more attention. While procedurally social media is generally treated no differently from other requests for production, parties often battle over relevance, proportionality, and burden.[35] Disputes may be avoided or mitigated by considering the following issues when assessing whether to preserve, how to request with specificity, how to search for, and how to produce social media evidence:

- which social media sources are likely to contain relevant information;
- who has power, possession, or control over the social media data;
- the date range of discoverable social media content;
- what information is likely to be relevant;
- the value of that information relative to the needs of the case;
- the dynamic nature of the social media and user-generated content;
- reasonable preservation and production formats; and
- confidentiality and privacy concerns related to parties and non-parties.

35. *Wilder v. Munro*, 2015 BCSC 1983 (CanLII) at para 16 ("the considerations for the court include the probative value of the information sought, privacy concerns, potential prejudice to the plaintiff and proportionality").

Some parties may also find it helpful to speak with opposing counsel before or during discovery planning[36] regarding the discoverable information that will be sought or should be provided from social media platforms and applications.[37]

The purpose of discovery planning 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.[38] 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;[39] the

---

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

37. On January 1, 2010, Ontario amended its Rules of Civil Procedure to include two new rules: Rule 29.1 (Discovery Plan) and Rule 29.2. (Proportionality in Discovery). Rule 29.1 imposes an affirmative obligation on the parties to agree to a discovery plan and requires that "[i]n preparing the discovery plan, the parties shall consult and have regard to the document titled *The Sedona Canada Principles Addressing Electronic Discovery* developed by and available from The Sedona Conference."

38. Drywall Acoustic, Lathing and Insulation, Local 675 Pension Fund (Trustees) v SNC Lavalin Group Inc., 2014 ONSC 660 at paras 81–84.

39. "Processing" means "the automated ingestion of electronically stored information into a program for the purpose of extracting metadata and text; and in some cases, the creation of a static image of the source ESI files according to a predetermined set of specifications, in anticipation of loading to a database. Specifications can include the de-duplication of ESI, or filtering based on metadata contents such as date or email domain and specific metadata fields to be included in the final product." "The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition" (2020) 21 Sedona Conf. J. 263 at 355. Processing can also involve steps to deal with documents that require special treatment, such as encrypted or

review and production of documents;[40] how privileged documents are to be handled or other grounds to withhold evidence; costs; and protocols.

This section is designed to provide guidance for addressing the most common discovery challenges associated with social media.[41]

A. Relevance and Proportionality

The scope of discovery for social media content is driven by a balance between relevance, proportionality,[42] and privacy interests. Relevance in discovery is broader than at trial. A consideration of relevance begins with the pleadings:[43]

> A party must produce every document that is relevant to the issues pleaded in the proceeding.

---

password-protected files. Parties should avoid making processing decisions that have consequences for others without first discussing those decisions. An effective discovery plan will address issues such as the means of creating hash values, whether to separate attachments from emails and which time zone to use when standardizing Date and Time values.

40. 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.

41. For additional guidance on these issues, see The Sedona Conference, "The Sedona Canada Principles Addressing Electronic Discovery, Third Edition, Public Comment Version" (2021) online: <https://thesedonaconference.org/publication/The_Sedona_Canada_Principles> ["The Sedona Canada Principles, Third Edition"], and The Sedona Conference, "Commentary on Legal Holds, Second Edition: The Trigger & The Process" (2019) 20 Sedona Conf. J. 341.

42. "The Sedona Canada Principles, Third Edition," *supra* note 41, Principle 4. Most Canadian jurisdictions have amended their respective rules of court to expressly include proportionality as a general rule for all litigation, and specifically in discovery procedures.

43. *Merpaw v. Hyde*, 2015 ONSC 1053 (CanLII).

> A litigant has the initial obligation of disclosing relevant documents in the first instance. There must be some evidence of non-disclosure or of omission from the production and disclosure obligations of the litigant before production will be ordered. The court is required to consider proportionality pursuant to Rule 29.2.03, and the evidence must suggest that the benefits of the investigation warrant the costs.
>
> The value of disclosure may be overborne by other values including privacy, access to justice and the fair and efficient use of scarce resources in the administration of justice. The court retains discretion and may refuse disclosure where information is of minimal importance but the search for it might compromise other important interests.[44]

The *Sedona Canada Commentary on Discovery of Social Media* does not identify all types of relevant social media evidence, as cases vary and social media sources are constantly evolving. Therefore, counsel should explore what social media their clients and opponents use and assess whether those sources of information may contain evidence relevant to the case. For example, even in a situation where social media evidence does not seem to impact issues of liability, it may be relevant to issues such as standing, damages, or good-faith participation in the judicial process. Because certain types of social media evidence can be readily destroyed (whether intentionally, unintentionally, or by a third party), counsel must take steps early in the case to assess the potential relevance of the client's social media

44. *Ibid*, paras 14–16.

content. Counsel must then help the client take reasonable steps to preserve it once a duty to preserve has been triggered.[45]

Courts generally reject efforts to obtain "all" social media postings or "entire" account data. This is because the entire contents of a social media source are not likely to be relevant in most cases, just as all of a party's emails are not likely to be relevant.[46] A court can refuse disclosure when the information is of little importance to the litigation and disclosure may constitute a serious invasion of privacy. The question to be asked is whether the invasion of privacy is necessary to the proper administration of justice, and if so, whether some terms are appropriate to limit that invasion.[47]

Social media presents some unique challenges to courts in their efforts to determine the proper scope of discovery or relevant information and maintaining proportionality. While it is conceivable that almost any post to social media will provide some relevant information concerning a person's physical and/or emotional health, it also has the potential to disclose more information than has historically occurred in civil litigation.[48]

Turning to proportionality, courts have repeatedly used the analogy that a computer hard drive is the digital equivalent to a filing cabinet. A request to be able to search a party's filing cabinet in the hopes that there might be found a document in which an admission against interest is made would clearly not be allowed—and its digital equivalent should also not be allowed.[49]

---

45. See Section III(C), *infra*.

46. *M.(A.) v. Ryan*, 1994 CanLII 6417; aff'd, 1997 CanLII 403 (SCC).

47. *Ibid*.

48. *Merpaw v. Hyde*, 2015 ONSC 1053 (CanLII).

49. *Ibid* at para 60.

As with all discovery, even if social media information may be relevant, efforts to preserve, collect, and produce should still be proportional to the needs of the case. Similarly, requests for social media evidence should be made with specificity and be proportional to the needs of the case.

1. Privacy Considerations

Privacy considerations impact both the scope and conduct of discovery involving social media evidence. Privacy obligations on parties arise from federal and provincial privacy statutes, as well as common law. These obligations require parties to consider individuals' privacy interests regardless of whether the individual is a party to the litigation. Such privacy interests are often a key consideration when dealing with social media evidence, given both the volume and sensitivity of personal information that exist on social media platforms. Individuals' privacy interests on social media and litigants' discovery rights require balancing. However, both can often be accommodated to a large extent by including practical solutions in the discovery planning process.

Privacy interests are not an automatic bar to discovery of relevant information, regardless of whether it is located in social media or elsewhere. Rather, privacy interests are best viewed as an important aspect of proportionality. Privacy concerns should not be confused with discovery exclusions such as legal privileges or doctrines recognized under well-developed case law. Just like these exclusions, a person's privacy interests in social media communications can influence the scope of discovery. However, unlike discovery exclusions, privacy interests are neither determinative nor binary in their impact. A party may not use privacy expectations as a blanket or categorical protection against discovery, but a party may use privacy interests to protect against overly broad or invasive discovery where privacy interests outweigh the probative value of the information

sought. Thus, requests for social media evidence should not be designed to harass or embarrass a party; nor should they be used as a tool to increase litigation costs.

Privacy considerations also have implications for the conduct of discovery. Statutory and common law privacy obligations impose requirements on how and when "personal information" should be collected, used, disclosed, and protected.

a. What is personal information?

The term "personal information" is broadly defined under Canadian privacy legislation as "information about an identifiable individual." Information will be "about" an individual when it relates to or concerns the individual.[50] Individuals will be "identifiable" where there is a serious possibility that they could be identified through the use of that information, alone or in combination with other available information.[51]

b. Statutory Privacy Landscape

Canada and its provinces, to varying extents, have public and private sector privacy legislation[52] governing the collection,

50. Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157 (CanLII), [2007] 1 FCR 203, at paras 43, 59, 61.

51. *Gordon v. Canada (Health)*, 2008 FC 258 (CanLII), at para 33.

52. 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

use, and disclosure of personal information that may affect the discovery process. The rest of this section focuses on the Canadian private sector privacy regime.

The privacy law regime under the federal Personal Information Protection and Electronic Documents Act (PIPEDA) applies to organizations that collect, use, or disclose personal information in the course of commercial activities.[53]

PIPEDA presumptively applies to all federally or provincially regulated entities, unless the organization is otherwise subject to provincial privacy legislation that has been declared to be "substantially similar" to PIPEDA.[54] The three provinces that have enacted "substantially similar" legislation are Alberta, British Columbia, and Québec. In such cases, the substantially similar provincial law applies instead of PIPEDA, although PIPEDA continues to apply to interprovincial or international transfers of personal information.[55]

Although the provincial statutes and PIPEDA share common objectives and are based upon similar key principles, there

---

of Privacy Act, RSPEl 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.

53. *PIPEDA*, *supra* note 52, c 5.

54. *Ibid* at s.26(2).

55. Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador have enacted privacy legislation as well, but only with respect to personal health information collected, used, or disclosed by health information custodians. These statutes should be consulted when a party to litigation (or third-party source of evidence) is a health information custodian or agent, and counsel anticipate that personal health information will be relevant to the issues in the case.

are some obligations imposed by the provincial statutes that exceed those imposed by PIPEDA.

The main area for uneven privacy law coverage between the federal and provincial statutes is in relation to employee personal information. PIPEDA only applies to information about employees of organizations that are federal works, undertakings, or businesses (as defined in PIPEDA).[56] In contrast, the privacy legislation in Québec, British Columbia, and Alberta applies to employee information held by organizations subject to these laws. As a result, organizations may face different privacy law considerations when handling social media evidence that contains, or constitutes, personal information of employees, depending on whether they are governed by federal or provincial law and whether they are deemed to be federal businesses under PIPEDA.

The prevailing view is that Canadian private sector privacy legislation does not apply to personal information collected for purposes of litigation. Further, while this legislation typically requires consent of and notice to an individual before their personal information is disclosed, disclosure required by the rules of court or a court or tribunal order is typically exempt.

Outside of the litigation context, an individual's consent is, with some exceptions, required for the collection, use, or disclosure of their personal information. Such consent may be implied in certain circumstances, but express consent is required for the collection, use, or disclosure of sensitive information and is encouraged by privacy regulators as a best practice in almost all cases. The central exemptions relevant to the litigation context are discussed below.

56. *PIPEDA*, *supra* note 52, s.2(1).

c. Privacy Law Exemptions Relevant to Civil Litigation

Provincial private-sector privacy laws each include a provision providing that nothing in those Acts shall be construed to interfere with information that is otherwise available by law to a party to a proceeding.[57] This prevents litigants from objecting to production of personal information contained in social media evidence relevant to the case.[58]

In contrast, PIPEDA does not contain a general exemption for information used in litigation, but the prevailing view is that PIPEDA does not apply to personal information handled in the course of litigation because litigation does not constitute a commercial activity. For example, if a defendant hires a private investigator to perform social media searches about the plaintiff, the defendant is not engaged in a commercial activity that engages PIPEDA, nor is any person employed by them doing so.[59] In contrast, if a federal business engages a background check service to perform social media searches before hiring a job candidate, the information will be subject to PIPEDA when used for hiring purposes. Importantly, however, if those social media search results become relevant to subsequent litigation, they

57. Personal Information Protection Act, SBC 2003, c 63, s.18(i); Personal Information Protection Act, SA 2003, c P-6.5, s.20(e); e Protection of Personal Information in the Private Sector [Québec's Private Sector Act] s.18.

58. Hatfield v. Intact Insurance Company, 2014 NSSC 232 (CanLII), at paras 25–30. See also *Pettigrew v. Halifax Regional Water Commission*, 2018 NSSC 197 (CanLII), at paras 26–27 for a similar conclusion respecting the application of the Nova Scotia Freedom of Information and Protection of Privacy Act in relation to the disclosure of third-party information.

59. State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada, 2010 FC 736 (CanLII), at para 106.

may be produced without consent if necessary, to comply with discovery obligations under the exemption described below.[60]

PIPEDA does contain certain exceptions to the requirement for consent that permit the collection, use, or disclosure of personal information that may apply in the litigation context. Of particular relevance, PIPEDA allows disclosure of personal information (1) to the organization's lawyer or notary;[61] (2) where required to comply with a court (or tribunal) order;[62] or (3) where required to comply with rules of court relating to document production.[63]

Given the exemption of litigation, statutory privacy law obligations are typically engaged for purposes and activities that extend beyond what is strictly required for the litigation. Examples of activities that may engage statutory obligations include collecting irrelevant personal information from social media pages, sharing information with U.S. counsel in parallel proceedings, and responding to access requests from likely litigants in advance of litigation.

Parties and their counsel should generally avoid the collection, use, or disclosure of personal information where it is unnecessary or unrelated to the litigation.

Parties and their counsel should also ensure that proper safeguards are incorporated into the collection, review, and disclosure of personal information from social media. Failure to apply

---

60. *Wyndowe v. Rousseau*, 2008 FCA 39 (CanLII), at paras 35–49. Kelly Friedman, "Canada's Privacy Regime as It Relates to Litigation and Trans-Border Data Flows" (2012) 13 Sedona Conf. J. 253 at 255–56 [*Friedman*] online: <https://thesedonaconference.org/sites/default/files/publications/253-266%20Friedman.pdf>.

61. *PIPEDA*, *supra* note 532, s.7(3)(a).

62. *Ibid* s.7(3)(c).

63. *Ibid*.

proper safeguards could give rise to privacy complaints if personal information is collected, reviewed, used, or disclosed where not strictly required by court rules or orders.

In addition, parties should be mindful of activities that may engage privacy laws in other jurisdictions. International privacy laws may apply to personal information on social media and may not have the same exemptions for litigation purposes.

d. Privacy Obligations and the Implied Undertaking Rule

The "implied undertaking rule" is a common law rule that prohibits parties from disclosing evidence and information obtained during the discovery process outside the confines of the litigation.[64] This rule has since been codified in various civil procedure rules and is referred to as the "deemed undertaking rule." Although this rule may lend comfort to litigants who are required to disclose personal details in the course of litigation but are concerned about broader dissemination of that information, the deemed undertaking rule does not provide full privacy protection. For example, in Ontario, the deemed undertaking rule only applies to evidence obtained in the discovery process and does not apply to evidence filed with the court or referred to during a hearing.[65] A court order can also be obtained to relieve compliance with the deemed undertaking rule.[66]

64. *Goodman v. Rossi* (1995), 24 OR (3d) 359 (Ont. C.A.). See *Friedman*, *supra* note 60, at 259–60 for a more extended discussion.

65. *Rules of Civil Procedure*, RRO 1990, Reg 194, r. 30.1.01.

66. *Rules of Civil Procedure*, RRO 1990, Reg 194, r 30.1.01. "The Sedona Canada Principles, Third Edition," *supra* note 41, Comment 9.c.

e. Common Law Privacy Issues Relevant to Social Media Evidence

Because social media is so easily used to communicate and create personal information, a party (or a party's employee) may have significant privacy concerns about the production of such evidence even if it is required by court rules and permitted by privacy statutes. In many cases it is necessary to balance privacy interests with discovery obligations even where consent to produce personal information is not required by statute. Similarly, privacy must be considered where no statute applies, such as for many organizations' employee information or data gathered outside the context of commercial or public-sector activity.

A privacy interest arises in information "that could qualify as revealing very personal information over which most right thinking Canadians would expect a reasonable expectation of privacy" or information that reveals "intimate details of the lifestyle and personal choices of the individual."[67] Although individuals' privacy interests may be diminished when they are parties to litigation, there are scenarios where privacy concerns will outweigh the need for full disclosure of relevant information in the judicial process.[68]

Common privacy concerns with social media include the form of access to the account information and the sensitivity of the communications. Because relevant information from social media accounts are documents for the purpose of discovery, social media evidence should be produced by the party with

---

67. *Carter v. Connors*, 2009 NBQB 317 (CanLII), at para 38.

68. Although obiter to the decision of the court, Justice McLachlin's (as she was then) comments in *M. (A.) v. Ryan*, 1997 CanLII 403 (SCC), [1997] 1 SCR 157, at paras 36–38 have been repeatedly cited by the courts in production cases, including those for social media content, for guidance in determining the appropriate balance to be struck when assessing a litigant's privacy interest in an application for production of documents.

control over it. It will generally never be necessary or appropriate to allow the opposing party to access a social media account directly or to require a litigant to provide their account password to another party. In rare cases where information about social media usage is relevant and cannot be obtained through production of documents or metadata from the accounts or associated devices, an expert should be engaged to perform a targeted review. Having a third party access the account or device, rather than providing a password and direct access to an opposing party or counsel, and permitting that expert to separate relevant information from data outside the scope of litigation or information belonging to non-parties minimizes the privacy intrusion.[69]

f. Litigants' Privacy Interests

In other cases, the content of documents subject to discovery will require significant balancing of parties' privacy interests with their rights to discovery. For example, the plaintiff in a case alleging nonconsensual distribution of intimate images may seek to avoid producing copies of the images themselves and propose to instead provide metadata about when the images were sent to the defendant or posted by the defendant to public websites. A court will first have to assess whether the content of the documents—the images themselves, in the above example—is relevant to the issues in the litigation. If relevance has been established, the court must then weigh the benefits of requiring the disclosure of the information against the invasion of privacy and the burden of production.[70] In assessing the weight to be

69. *Bishop v. Minichiello*, 2009 BCSC 358 (CanLII), at paras 46–58, leave to appeal for further production dismissed, 2009 BCCA 555.

70. *Leduc, supra* note 2, at paras 14, 32–36; *Frangione, supra* note 2, at paras 26–73; *Murphy, supra* note 2, at para 10; *McDonnell, supra* note 2, at paras 15–16; and *Casco*, *supra* note 2, at para 2.

given to the privacy interest in a particular case, courts have generally sought to assess "whether the invasion of privacy is necessary to the proper administration of justice and, if so, whether some terms are appropriate to limit that invasion."[71] For example, where there is risk that an opposing party will misuse the personal information contained in certain productions, an order restricting access to counsel only may be appropriate.

Some courts have found litigants' privacy interests in social media posts to be limited, even where the documents are on a restricted access page, because the act of sharing materials on social media undercut the assertion of a privacy interest.[72] A number of decisions, however, have expressed a contrasting view: by restricting access or setting a social media page to private, a party has indicated a choice to exclude all other users. From this choice, the courts inferred that a litigant retains a "real" privacy interest in the content of the restricted access site.[73] This is consistent with the conception of privacy rights based on the individual's discretion to control, not simply to hide, their personal information.[74] It is also consistent with the

71. *A.M. v. Ryan*, 1994 CanLII 6417 (BC CA), at para 45; see also *Merpaw v. Hyde*, 2015 ONSC 1053 (CanLII), at para 20.

72. The most extreme statement of this view was made by the court in *Murphy, supra* note 2, when it concluded at para 20 that "[t]he plaintiff could not have a serious expectation of privacy given that 366 people have been granted access to the private site." See also, for example, *Leduc*, *supra* note 2, at para 35, and *Frangione, supra* note 2, at para 38.

73. See S*tewart v. Kempster*, 2012 ONSC 7236 (CanLII), at para 24. See also *Jones v. I.F. Propco*, 2018 ONSC 23 (CanLII), at para 41.

74. This issue has been addressed in detail in the criminal law and Charter privacy rights context. For example, the Supreme Court in *R. v. Marakah*, 2017 SCC 59 (CanLII), and *R. v. Jones*, 2017 SCC 60 (CanLII), made it clear that a party can have a reasonable expectation of privacy in their digital communications even if the information has been sent to another, such as by text message. Therefore, charter privacy rights of individuals vis-à-vis the state do

common law development of privacy torts in Canada, several of which focus on the individual's right to control the forum and scope of access to and disclosure of their personal information.

g. Third-Party Privacy Interests

Courts have not hesitated to order production of content from social media platforms even in the absence of the consent of the third party. However, where the social media content contains personal information that is not relevant or where their privacy interest outweighs factors favouring disclosure, courts have ordered that the information be redacted or otherwise concealed to protect the third party's privacy interest.[75] This balancing exercise may also result in the severance of different parts of social media evidence. For example, a court may order production of a posted photograph that depicts third parties but permit the comments on such a photo to be withheld on the basis of privacy concerns and relevance.[76]

Third-party interests also arise where social media evidence is no longer in the control or possession of any party and must be obtained from the social media platform or provider. In such cases, a party may seek a Norwich order for pre-discovery production from third parties. This may be necessary to give the third party comfort that it is legally permitted to disclose personal information in its possession without consent of the subjects. In assessing such applications, courts weigh a variety of

not depend on the complete nondisclosure of personal information; an individual may selectively disclose private details via social media to some while maintaining privacy rights over that information against others.

75. *Fric v. Gershman*, 2012 BCSC 614 (CanLII), at para 72.

76. *Ibid* at para 75, citing Dosanjh v. Leblanc and St. Paul's Hospital, 2011 BCSC 1660.

factors, including the privacy interests of the person whose information is to be disclosed.[77]

h. Best Practices

Parties and their counsel should anticipate litigant and third-party privacy concerns at the outset of the discovery planning process and raise them with opposing counsel well in advance of production. Agreements on privacy-accommodating steps should be memorialized in the discovery plan, or otherwise in writing. In many cases the parties will be aligned on the appropriate steps to avoid unnecessary invasions of privacy, or the issues can be streamlined to reduce costs associated with seeking court direction.

Practical solutions can often accommodate both discovery rights and privacy interests of litigants and third parties. Reviewing metadata only or disclosing information on a "counsel's eyes only" basis are two examples discussed above. Other examples include permitting parties to redact or sever sensitive and irrelevant information from documents being produced; restrictions on filing information in court without notice; and data security practices including requirements to destroy information after the matter has ended.

Counsel should also consider whether case-specific privacy issues meet the *Sierra Club* test for a confidentiality order and

77. The court in *York University v. Bell Canada Enterprises*, 2009 CanLII 46447 (ON SC), weighed five factors in assessing York University's application for a Norwich Order to have Bell and Rogers disclose information necessary to identify the anonymous author(s) of allegedly defamatory emails and a web posting, including at paragraphs 29-36 whether the interests of justice when set against competing interests such as a customer's expectation of privacy favour obtaining the disclosure. See also *Carleton Condominium Corporation No. 282 v. Yahoo! Inc.*, 2017 Carswell Ont 10986 at paras 15–19.

the high value courts assign the open court principle.[78] Parties should not assume that simply because they agree to designate documents containing personal information as confidential the court will seal them from public access. Alternative measures—including modifying documents to render them less sensitive, producing or filing different evidence, or agreeing to uncontested facts that render the personal information unnecessary—should be considered and discussed with all parties early in the discovery and trial preparation phases of litigation.

The same considerations regarding litigants' privacy interests apply to discovery of third-party information. While parties may pursue discovery of relevant social media content regarding third parties,[79] they should consider managing the discovery to minimize potential embarrassment to third parties and protect against unnecessary disclosure of their sensitive personal information.[80] Counsel should assess the scope of third-party information, its sensitivity, and whether it is intertwined with discoverable social media content such that it is part of relevant social media information to be produced. If intertwined sensitive third-party information exists, counsel should consider proactively addressing these issues through a good-faith attempt to confer. Parties may seek to limit or set the circumstances for disclosure of sensitive information of third parties contained in social media content by incorporating procedures for producing, transferring, storing, or using such information as evidence.

---

78. Sierra Club of Canada v. Canada (Minister of Finance), 2002 SCC 41 (CanLII), [2002] 2 SCR 522.

79. See *Frangione, supra* note 2, (holding that an inference could be made from the plaintiff's Facebook profile that private messages with Facebook friends were likely relevant).

80. See *Carter v. Connors*, 2009 NBBR 317 (QB) (holding that document production should not trench upon third-party privacy rights).

2. Requesting Social Media Evidence

The appropriate procedure for requesting and obtaining relevant social media information, as with all types of electronically stored information (ESI), is for the requesting party to draft requests with specificity and for the responding party to conduct a reasonable inquiry, assert reasonable objections, and produce relevant, responsive nonprivileged information.[81]

The duty of reasonable inquiry regarding relevant social media—as with all relevant evidence—begins with the responding party's compliance with its initial disclosure obligations.[82] The responding party must also conduct a reasonable inquiry once served with properly issued requests for production of documents. A requesting party has no obligation to prove relevant social media evidence exists or is publicly available before a responding party's duty to conduct a reasonable inquiry is triggered.[83]

---

81. *Merpaw v. Hyde*, 2015 ONSC 1053 (Ont. Sup. Ct. J.) (stating that the defendant must establish evidence of omission of relevant documents).

82. Rules of Civil Procedure, RRO 1990, r. 30.02(1); Court of Queen's Bench Rules, Man Reg 553/88, r. 30.02(1); Rules of Court of New Brunswick, NB Reg 82-73, r. 31.02(1); Rules of the Supreme Court of the Northwest Territories, NWT Reg R-010-96, r. 219; Rules of Civil Procedure, PEI Rules, r. 30.02(1); Supreme Court Civil Rules, BC Reg 168/2009, r. 7-1(1); Alberta Rules of Court, Alta Reg 390/68, r. 187.1(2); Rules of the Supreme Court, 1986, SN 1986, r. 32.01(4); Nova Scotia Civil Procedure Rules, NS Civ Pro Rules 2009, r. 14.08(2); The Queen's Bench Rules, Sask QB Rules 2013, r. 5-6(2); Rules of Court, Yuk Reg OIC 2009/65, r. 25(3).

83. Rules of Civil Procedure, RRO 1990, r. 30.02(2); Court of Queen's Bench Rules, Man Reg 553/88, r. 30.02(2); Rules of Court of New Brunswick, NB Reg 82-73, r. 31.02(2); Rules of Civil Procedure, PEI Rules, r. 30.02(2); Alberta Rules of Court, Alta Reg 390/68, r. 205; Rules of the Supreme Court, 1986, SN 1986, r. 32.02; Nova Scotia Civil Procedure Rules, NS Civ Pro Rules 2009, r. 14.10; The Queen's Bench Rules, Sask QB Rules 2013, r. 5-6(2); The Queen's Bench Rules, Sask QB Rules 2013, r. 5-11; Rules of Court, Yuk Reg OIC 2009/65, rr. 25(3)-(4); Supreme Court Civil Rules, BC Reg 168/2009, r. 7-1(13);

Upon determining that the preservation of social media evidence is necessary,[84] the parties should discuss the requirement during the discovery planning stage. Specifically, the parties should communicate to the affected persons the need to preserve relevant social media information. This notice is referred to as a "legal hold" or preservation notice.[85] The style, content, and distribution of the legal hold 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 should set out in detail the kinds of information that must be preserved so the affected custodians can preserve it. The legal hold should mention the volatility of social media content and make it clear that particular care must be taken not to alter, delete, or destroy it.[86]

Rules of the Supreme Court of the Northwest Territories, NWT Reg R-010-96, r. 225.; Leduc v. Roman, [2009] OJ No 681 (Ont. Sup. Ct. J.) ("A party who maintains a private, or limited access, Facebook profile stands in no different position than one who sets up a publicly-available profile. Both are obliged to identify and produce any postings that relate to any matter in issue in an action.").

84. 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.

85. "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.

86. Ontario Bar Association, *Model Precedents*, online: <https://www.oba.org/EIC/Model-Precedents>.

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

Although there is no specific obligation to preserve electronic documents in advance of litigation,[87] the Superior Court has recognized the existence of an implicit obligation to preserve evidence based on the general obligation of parties to refrain from acting with the intent of causing prejudice to another person or behaving in an excessive or unreasonable manner, which would be contrary to the requirements of good faith as prescribed by the *Code of Civil Procedure*.[88]

Before litigation has started, a party who has reason to fear that relevant evidence will become lost or more difficult to use can apply to the court for an order to allow a person of the party's choice to examine the evidence in question if its condition may affect the outcome of the expected legal proceeding.[89]

In Québec, in view of the absence of an express preservation obligation, a party seeking a preservation order would need to present a motion for injunction or safeguard order in accordance with the criteria governing such proceedings.[90] In all circumstances, parties should send a legal hold letter to the other

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

88. Québec Code of Civil Procedure, CQLR c C-25, s 4.1.

89. *Ibid*, s 438.

90. *Ultramar, supra* note 87, at para 26.

parties to ensure that the other parties are aware of the ESI[91] that will be requested.

Social media evidence is often sought in cases where a party's physical or mental state during a period is relevant. In cases where physical ability, mental condition, or quality of life are at issue, social media postings reflecting physical capabilities, state of mind, or changes in a party's circumstances may be relevant and discoverable.[92] Such information has been found to be relevant in criminal proceedings, employment discrimination, personal injury, and workers compensation cases. In all cases courts must assess whether evidence from social media may reveal some insight into the crime or credibility of the witness, weighing whether the evidence is more probative than prejudicial.[93]

B. Possession, Custody, and Control

Whether relevant social media information is in the responding party's possession, custody, or control is another threshold issue for assessing whether there is a duty to preserve or produce such information.[94] A party who uses social media may not

---

91. Electronically stored information, regardless of the media or whether it is in the original format in which it was created, as opposed to stored in hard copy (i.e., on paper).

92. *See Jones v. I.F. Propco*, 2018 ONSC 23 (Ont. Sup. Ct. J.); *Stewart v. Kempster*, 2012 ONSC 7236 (Ont. Sup. Ct. J.); *Papamichalopoulos v. Greenwood*, 2018 ONSC 2743 (Ont. Sup. Ct. J.) (photos at odds with the plaintiff's allegedly severe and permanent injuries are relevant and producible).

93. *R. v. Seaboyer*, [1991] 2 SCR 577 (preventing inflammatory statements or embarrassing photographs from distracting the court), *R. v. Jilg*, 2010 BCSC 1476.

94. The concept of possession, control, or power, as addressed herein, derives from *Alberta Rules of Court*, Alta Reg 390/68, r 193(1); *Alberta Rules of Court*, Alta Reg 124/2010, r 5.14(1); *Supreme Court Civil Rules*, BC Reg 168/2009, rr 7-1(10), 7-1(15); *Court of Queen's Bench Rules*, Man Reg 553/88, rr

have "possession" of the data, except to the extent that some of the data may be on the party's devices.[95] That social media technologies are constantly changing their functionality and storage features adds to the complexity of this issue.

1. "Control" By Individual Parties

A party generally has possession, custody, or control over its social media content. Other than certain controls implemented by the social media provider, the account user largely controls the content created on the account, the timing of when the content is posted, the deletion of content from the account, the other users who can view content posted to the account, and the like.[96] Thus, while some of the content may be exclusively obtainable from the social media provider's systems, the user still controls the vast majority of information shared via the account and can

30.04(1), 30.04(3); *Rules of Court of New Brunswick*, NB Reg 82 82-73, r 31.04; *Rules of the Supreme Court of the Northwest Territories*, NWT Reg R-010-96, r 225(1); *Rules of the Supreme Court*, SN 1986, r 32.05; *Nova Scotia Civil Procedure Rules* (1972), NS Civ Pro Rules 2009, rr 14.10, 16.02, 20.04; *Rules of Civil Procedure*, RRO 1990, r 30.04; *Rules of Civil Procedure*, PEI Rules, r 30.04; *The Queen's Bench Rules*, Sask QB Rules 2013, rr 5-11(1), 5-11(3); *Rules of Court*, Yuk Reg OIC 2009/65, r 25(18). *Rules of Civil Procedure*, RRO 1990, r 30.04 states "[a] party who serves on another party a request to inspect documents (Form 30C) is entitled to inspect any document that is not privileged and that is referred to in the other party's affidavit of documents as being in that party's possession, control or power." The occasional use of "*and* power" in the *Commentary* is intended to address all three factors. It does not replace or diminish the "possession, control, or power" standard, which is discussed in this Section.

95. See The Sedona Conference, "Commentary on Rule 34 and Rule 45 'Possession, Custody, or Control'" (2016) 17 Sedona Conf. J. 467 at 524.

96. *Leduc v. Roman*, [2009] OJ No 681 (Ont. Sup. Ct. J.) at para 32 ("A party who maintains a private, or limited access, Facebook profile stands in no different position than one who sets up a publicly-available profile. . . . Mr. Leduc exercised control over a social networking and information site to which he allowed designated "friends" access.").

often take steps to preserve and collect information from the account. Further, the user can do so without violating the service provider's terms of service or provincial or federal law (such as PIPEDA).

For example, an individual user may generate content by typing text, uploading files, or live-recording video or audio content to a social media account from a mobile device or computer. To the extent the content was uploaded from physical storage on that or another device, the content may still reside on the device and thus likely remains in the user's possession, regardless of whether a second copy may also reside on the servers of the social media provider. Similarly, content created on a smartphone application may be stored in that application on the phone—again, remaining in the user's possession. Thus, locally stored copies of uploaded content remain in the user's possession, custody, or control.

This distinction does not suggest that posted content to a social media account is not in and of itself a unique piece of discoverable evidence. It may be meaningfully different from a locally stored copy.

Similarly, evidence that posted content was removed from a social media account, the timing of when the account was updated or deactivated, or other account activity may be relevant to a given case. Records of such account activity are often in the possession of the social media provider.[97] Nevertheless, the user

97. Account activity log data may include the date and time the account was accessed, internet protocol (IP) addresses from where the account was accessed, and reports detailing other aspects of the user's social media account. *Carter v. Connors*, 2009 NBBR 317 (QB) ("It is not clear at this point whether Bell-Aliant has the capacity to generate discrete Facebook use data and the requested order is conditional on those records being in existence or able to be specifically identified and generated."); *Conrod v. Caverley*, 2014

may still exercise "control" over such information and may be able to gain, grant, or deny access pursuant to end-user agreements, social media provider policy,[98] or as a "customer" of or

NSSC 35 (SC) (stating that usage records were relevant and the contents did not reveal any potentially sensitive personal information).

98. See, *e.g.*, *Facebook Terms of Service* § 3, online: Facebook <https://www.facebook.com/legal/terms/update> (last revised 22 Oct. 2020) ("You own the intellectual property rights (things like copyright or trademarks) in any such content that you create and share on Facebook and the other Facebook Company Products you use. Nothing in these Terms takes away the rights you have to your own content. You are free to share your content with anyone else, wherever you want."); *Twitter Terms of Service* § 3, online: Twitter <https://twitter.com/en/tos> (effective 19 Aug. 2021) ("You retain your rights to any Content you submit, post or display on or through the Services. What's yours is yours — you own your Content (and your incorporated audio, photos and videos are considered part of the Content."); *Instagram Privacy and Safety Center, Terms of Use* § 4, online: Instagram Help Ctr. <https://help.instagram.com/478745558852511> (last revised 20 Dec. 2020) ("We do not claim ownership of your content that you post on or through the Service and you are free to share your content with anyone else, wherever you want."); *LinkedIn User Agreement* § 2.2, online: LinkedIn <https://www.linkedin.com/legal/user-agreement> (effective 11 August 2020) ("As between you and others (including your employer), your account belongs to you. However, if the Services were purchased by another party for you to use (e.g. Recruiter seat bought by your employer), the party paying for such Service has the right to control access to and get reports on your use of such paid Service; however, they do not have rights to your personal account."); *Snap Inc. Terms of Service, Rights you Grant Us* § 3, online: Snap <https://www.snap.com/en-US/terms/> (effective 30 Sept. 2021) ("Many of our Services let you create, upload, post, send, receive, and store content. When you do that, you retain whatever ownership rights in that content you had to begin with."); *Reddit User Agreement* § 4, online: Reddit <https://www.reddit inc.com/policies/user-agreement> (last revised 12 Aug. 2021) ("You retain any ownership rights you have in Your Content, but you grant Reddit the following license to use that Content . . . ."); *Tumblr Terms of Service* § 6, online: Tumblr <https://www.tumblr.com/policy/en/terms-of-service> (last modified 21 July 2021) ("Users retain ownership and/or other applicable rights in User Content, and Tumblr and/or third parties retain ownership

"subscriber" to the account.[99] As noted in more detail below, most social media platforms have established means by which a user can download content (data) from the platform.

An account user's "ownership," i.e., legal right, to its social media content may be confirmed by the social media provider's terms of service. Some social media providers specify in their terms of use that a user maintains control of its own content. Even where the service provider is silent on the issue of control or ownership over the account, the user's valid authorization may be required for anyone other than the user to obtain content from the account. In other words, an account user likely has a legal right to obtain its social media information from the service provider because it is a customer of or subscriber to the social media service.

Thus far, courts have not expressly applied the practical ability test to an individual's ability to obtain the social media information of another entity or party. Nevertheless, a few courts in the United States have found control—without specifically invoking the practical ability test—despite the individual not having a legal right to the requested information.[100]

---

and/or other applicable rights in all Content other than User Content. You retain ownership you have of any intellectual property you post to Tumblr.").

99. See *infra* Section III(D).

100. See, *e.g.*, *Meyer v. DG Retail LLC*, No. 13-2115-KHV, 2013 WL 5719508 (D. Kan. Oct. 21, 2013) (compelling a plaintiff to produce a job posting she found on a social media site despite the fact that it was not posted by her, nor did it originate from her own Facebook page); *contra Fox v. Pittsburg State Univ.*, No. 14-2606-JAR-KGG, 2015 WL 7572301, at *2 (D. Kan. Nov. 24, 2015) (declining to compel the social media postings of the non-party husband of a plaintiff because plaintiff did not have possession, custody, or control over the husband's internet postings).

2. "Control" by Organizational Parties

The determination whether an organization has possession, custody, or control of social media content stored on its internal servers and infrastructure is similarly straightforward. A corporation has the "ultimate authority to control, to add, to delete, or modify" content it creates and stores on either its own servers or on those of a third party.[101]

Employers generally do not have control over their employees' personal social media accounts. Personal property of an employee is not generally under the "control" of the employer unless the employer has a legal right to obtain the property from its employee.[102]

An employer's attempt to solicit social media usernames and passwords from its employees to facilitate social media access and collection by the employer may violate certain laws. Moreover, provincial and federal statutes may limit an employer's ability to implement policies concerning employees' use of social media. Even if an employee were to leave social media access credentials on an employer-issued computer, the employer would still likely be prohibited from using such credentials to access the account.[103] And employers do not have "control" over something that they are prohibited from accessing by law.

---

101. Red Label Vacations Inc. v. 411 Travel Buys Ltd., 2015 FC 18.

102. See *Canadian Broadcasting Corporation v Canadian Media Guild*, 2021 CanLII 761 (CA LA); *R v. Cole*, 2012 SCC 53 (holding that employees have a reasonable expectation of privacy in their work computers where personal use is permitted or reasonably expected).

103. *Canadian Broadcasting Corporation v. Canadian Media Guild*, 2021 CanLII 761 (CA LA) (holding that an employee's manager was not permitted to search private social media accounts inadvertently left logged into on a shared work laptop).

3. "Control" by Third Parties

While certain discoverable information may be visible to a party through its social media account, it may be removed by a third party (who created, posted, and potentially controls that information) or the social media provider. The account holder frequently cannot demand access to the removed content because it was not created by the account holder.

C. Preservation, Collection, and Search Obligations Generally

The popularity of social media, the proliferation of new technologies, and their rapid adoption by the public have made its preservation and collection more complicated than in many areas of discovery. Moreover, the dynamic nature of social media mandates that parties be proactive in addressing preservation.

1. Considerations for Preserving and Collecting Social Media

As with other forms of evidence, the preservation obligation with respect to social media information arises when a party knows or reasonably should know that it is relevant to actual or reasonably anticipated litigation.[104] Once the preservation obligation arises, a party should determine what sources of social media within its possession, custody, or control may contain information relevant to the litigation. The existence of an information retention policy that a party consistently observes can be a great aid in this preservation effort.[105]

---

104. See *Blatherwick v. Blatherwick*, 2015 ONSC 2606 at paras 295–97, 560–62 (defendant found in breach of Mareva Order that required he preserve relevant electronic documents after emails had been automatically deleted).

105. See The Sedona Conference, "Commentary on Proportionality in Electronic Discovery" (2017) 18 Sedona Conf. J. 141, 152 (observing in Principle 1 that information retention policies, among other protocols, can help a party satisfy preservation duties).

Social media raises a number of preservation and collection issues that may need to be addressed in connection with a review of a party's preservation obligations. As an initial matter, a party needs to know exactly what social media is to be preserved and collected that is within its possession, custody, or control.[106] For example, a party might need to collect its relevant ESI from a third-party social media provider to avoid its potential loss, particularly if the provider could take action to terminate the account and delete content.

The dynamic nature of the social media market—in which providers quickly fluctuate from success to failure—often leads to providers going out of business. In such instances, the responding party has to determine if its data is still available and whether it can be retrieved. Where the social media entity simply stops providing service, that entity should inform users whose data it holds accordingly so that arrangements can be made to provide users with their data. If the responding party cannot obtain or access its data due to a provider's insolvency, that data may no longer be in the party's possession, custody, or control.

A party should also consider the types of social media data that may be obtained, which may go beyond ESI that would ordinarily be accessible to a user on a social media platform. Data obtained from the provider could include geographical coordinates from image files or other sources, hashtags, referral links, payment history, lists of friends or followers, along with unusual language abbreviations and purposeful misspellings. It could also encompass other content such as emojis used in text messaging and live or streamed video data. Whether such information needs to be preserved depends on its relevance and

106. See *supra* Section III(B).

proportionality.[107] Features such as encryption and ephemeral messaging can also raise preservation issues that need to be considered in any review of social media data.[108]

Next, the party should consider whether it needs the services of a third-party vendor to help preserve or collect relevant social media content. The value of the case and the nature of the issues will likely affect this determination. In addition, a party may need different technologies to collect diverse content types from the variety of social media outlets where discoverable information may reside. Technical sophistication may be required to load the collected data onto a platform for review. The cost of preservation and collection is also a factor, as the range of services available differs for various services and budgets.[109]

A party should additionally consider whether the dynamic nature of a social media platform requires that it perform more than one collection from that platform. If the social media content as of a particular point in time is relevant to a matter, then it may be advisable to seek to extract the social media data at that time. In other instances, it may be appropriate to make collections at periodic intervals.

Finally, the party must also consider the evidentiary aspects of preservation and collection, as authentication of social media evidence has been an ongoing issue over the years.[110]

---

107. See *supra* Section III(A).

108. See *supra* Section II(B)(3).

109. See "Commentary on Proportionality in Electronic Discovery," *supra* note 105, at 174–75 (discussing in Principle 6 that parties should have the discretion to select technologies that address their discovery needs).

110. See *infra* Section V.

2. The Role of Cooperation

Parties should consider working with litigation adversaries to develop reasonable steps for identifying and handling difficult social media preservation and collection issues.[111] Such discussions will ideally take place as early as possible and should be raised prior to or during discovery planning. Relevance and proportionality principles should guide those discussions, with parties seeking to reach a resolution that satisfies their respective needs. This obligation may include mutual steps to preserve social media ESI, consideration of other ESI sources addressing the same issues that would obviate the need to preserve the social media, or the use of other evidentiary tools (e.g., stipulations or phased discovery to determine what is available from other sources).

Even if discussions between counsel are ultimately unsuccessful at this stage, the parties have at least framed the issues for further consideration and possible resolution by the court.[112] There will undoubtedly be instances where such cooperation may not be possible (as when opposing counsel has not been identified after the duty to preserve is triggered) or practicable (when an adversary is unreasonable).[113]

---

111. See "The Sedona Conference Cooperation Proclamation" (2009 Supp.) 10 Sedona Conf. J. 331; As noted above, as an example, under the Ontario Rules of Civil Procedure (Rule 29.1), all parties to an action must agree to a discovery plan if they intend to obtain evidence through documents, oral examination or examination for discovery by written questions. A discovery plan outlines the scope of the discovery for all parties and is meant to be a collaborative process which assists in moving the legal proceeding forward.

112. See "Commentary on Proportionality in Electronic Discovery," *supra* note 105, at 155–59 (explaining in Principle 2 the roles of cooperation and phased discovery in advancing the aims of proportional discovery).

113. See The Sedona Conference, "Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible" (2009) 10 Sedona Conf. J. 281.

3. The Interplay Between Reasonable Steps and Social Media

The touchstones of relevance and proportionality inform both the scope and nature of preservation of social media, with questions regarding the adequacy of a party's preservation efforts being a fact-based inquiry. Each party has an obligation to take reasonable steps to preserve, disclose, and produce any document the party's possession, power, or control that the party knows exists and knows is relevant to the action.[114]

Canadian courts have repeatedly held that ESI is producible and compellable in discovery.[115] Rules of court make relevancy

---

114. *Rules of Civil Procedure*, RRO 1990, O Reg 194, r 30; *Alberta Rules of Court*, Alta Reg 124/2010, Part 5; *Supreme Court Civil Rules*, BC Reg 168/2009, r 7-1; *Court of Queen's Bench Rules*, Man Reg 553/88, r 30; *Rules of Court*, NB Reg 82-73, r 31; *Rules of the Supreme Court*, SNL 1986 c 42, Sch. D, r 32; *Rules of the Supreme Court of the Northwest Territories*, NWT Reg 010-96, Part 15; *Rules of the Supreme Court of the Northwest Territories*, NWT Reg 010-96 (Nu), Part 15; *Nova Scotia Civil Procedure Rules,* Royal Gazette Nov 19, 2008 at r 16; *Supreme Court Rules of Civil Procedure*, Prince Edward Island, r 30; *The Queen's Bench Rules*, Sask. Gaz. December 27, 2013, 2684, Part 5; *Rules of Court*, YOIC 2009/65, r 25; *Tax Court of Canada Rules (General Procedure)*, SOR/90-688a, rr 78-91; and *Federal Courts Rules,* SOR/98-106, rr 222- 233.

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

The general rules requiring documentary production are found at the following sections in the relevant province's rules: *Ontario Rules of Civil Procedure*, RRO 1990, O Reg 194, r 30.02 [*Ontario Rules*]; *Alberta Rules of Court*, Alta Reg 124/2010, Part 5 [*Alberta Rules*]; *British Columbia Supreme Court Civil Rules*, BC Reg 168/2009, r 7-1 [*BC Rules*]; *Manitoba Court of Queen's Bench Rules*, Man

a prerequisite to production, regardless of the form of record. For example, Part Five, Rule 5.2(1) of the *Alberta Rules of Court*[116] provides that producible records be both relevant and material. The Ontario *Rules of Civil Procedure*[117] 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.[118]

The "reasonable steps" standard calls for a good-faith assessment of what data may be relevant to the claims or defenses in the litigation. Generally, once evidence is in a party's possession and control, they have an obligation to preserve it until trial.[119] In the context of social media, "reasonable steps" should be

---

Reg 553/88, r 30.02 [*Manitoba Rules*]; *New Brunswick Rules of Court*, NB Reg 82-73, r 31.02 [*NB Rules*]; *Newfoundland and Labrador Rules of the Supreme Court*, SNL 1986 c 42, Sch. D, r 32.01 and 32.04; *Northwest Territories Rules of the Supreme Court*, NWT Reg 010-96, r 219, 225 and 229 [*NWT Rules*]; *Nunavut Rules of the Supreme Court*, NWT Reg 010-96 (Nu) r 219, 225 and 229 [*Nu Rules*]; *Nova Scotia Civil Procedure Rules*, Royal Gazette Nov 19, 2008 at r 16. [*Nova Scotia Rules*]; *Prince Edward Island, Supreme Court Rules of Civil Procedure* [*PEI Rules*] , r 30.02; *Saskatchewan The Queen's Bench Rules*, Sask. Gaz. December 27, 2013, 2684, Part 5 [*Saskatchewan Rules*]; *Québec Code of Civil Procedure*, CQLR c C-25, s 401-403 [*Québec Code*]; *Yukon Rules of Court*, YOIC 2009/65, r 25 [*Yukon Rules*]; *Tax Court of Canada Rules (General Procedure)*, SOR/90-688a, r 78 and 80 [*Tax Court Rules*]; and *Federal Courts Rules* (SOR/98-106), r 222 and 223.

116. *Alberta Rules*, *supra* note 115.

117. *Ontario Rules*, *supra* note 115, 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.

118. See *BC Rules*, *supra* note 115.

119. *R. v. Prosa*, 2015 ONSC 3122 (Can LII). Rules in the various Canadian provinces and territories refer to the concept of possession, custody, and control differently. As an example, in Alberta, the term "possession, power, and control" is used. See footnote 94.

examined through the additional lens of unique social media discovery challenges. Those challenges include that social media is often hosted remotely, may include data that is difficult to access, is dynamic and collaborative by nature, can include several data types, often involves privacy issues, and frequently must be accessed through unique interfaces. Any subsequent court review of the reasonableness of a party's preservation actions should use as its frame of reference the party's knowledge at the time preservation decisions were made.[120]

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

In considering preservation issues, it may be that some social media and information sources are more difficult or more

120. See "Commentary on Proportionality in Electronic Discovery," *supra* note 105, at 151; "The Sedona Canada Principles, Third Edition," *supra* note 41, Comment 3.a; *Culligan Canada Ltd. v. Fettes*, 2009 SKQB 343 at para 87 (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."

expensive to preserve than others. If a party can conduct an inventory of the relevant information in its possession, custody, or control, then it may be in a position to determine if certain ESI is duplicative and, if so, which sources it should focus on preserving. In any such exercise, cost is a legitimate consideration.[121]

Documenting the preservation process, including identifying relevant social media information and a party's decisions, can be helpful in establishing a defensible process. This is particularly the case as spoliation disputes may arise years after the original preservation efforts. Such a document should be updated as circumstances change; identifying, for example, the changed conditions and new actions taken.

4. Means of Preservation and Collection of Social Media

The available tools for preserving and collecting social media are becoming more sophisticated, more varied, and continue to evolve with changing technology. Thorough documentation and verification of the process and results will help ensure that evidence supporting the decisions and actions taken during the process is available to rebut spoliation claims that may arise in long-running litigation.

a. Static Images

Some practitioners resort to capturing static images of social media data (i.e., screen shots and PDF images) as a means of preservation.[122] Printing out social media data has its

121. See "The Sedona Canada Principles, Third Edition," *supra* note 41, Principle 2 (stating that "in any proceeding, steps taken in the discovery process should be proportionate, taking into account: . . . (v) the costs, burden and delay that the discovery of the ESI may impose on the parties.").

122. See *infra* Section V; *R. v. Mills*, 2019 SCC 22 at paras 53–57 (screenshots of Facebook and email messages admissible and not a breach of privacy); *R.*

evidentiary limitations, as a static image does not capture the metadata of the image, other than whatever information may be viewable as part of the screen shot. As a result, static images may result in an incomplete and inaccurate data capture that is hard to authenticate, except on the basis of the personal knowledge of a witness.[123] Social media may also contain data and content, such as video, that cannot be properly collected in the form of static images.[124] In addition, social media outlets use different interfaces to display content, further complicating efforts to create standardized snapshots.[125] Any such collection will most likely be a visual representation that does not include metadata, logging data, or other information that would allow the content to be easily navigated and used.[126]

---

v. Martin, 2021 NLCA 1 at paras 29, 70–71 (screenshots of Facebook posts were admissible as there was no allegation the screenshot software altered their contents).

123. See *R. v. Hirsch*, 2017 SKCA 14 at para 18; Hon. Paul Grimm, Gregory Joseph & Daniel Capra, "Best Practices for Authenticating Digital Evidence" (2016) West Acad. Pub. (discussing circumstances in which static evidence of social media can be authenticated). See also *R. v. Bernard*, 2016 NSSC 358 at para 58 (evidence inadmissible based on the absence of evidence as to the origin of the screenshots); *R. v. Ball*, 2019 BCCA 32 (fact that photographed Facebook messages were admitted without testing their admissibility part of finding of miscarriage of justice).

124. Depending on the specific type of information that needs to be preserved or collected, videoing/interactive demonstration software that creates a record of the experience of navigating a site may more accurately represent the dynamic nature of the information, including capturing dynamic and nontext postings such as audio and video materials.

125. For example, Facebook uses algorithms based on a subscriber's prior usage to determine how to array the web content.

126. Circumstantial evidence may enhance authentication, including the presence of photographs, email addresses, and posting dates. See, *e.g.*, *R v. Durocher*, 2019 SKCA 97 at paras 47–50. Related data obtained from other sources, including email notifications of posting activity and computer and account usage logs, may provide additional context to aid authentication.

While recognizing these limitations of static images as a means of preservation, their use may be appropriate in situations in which the visual representation of certain data is essential or sufficient (e.g., capturing a photograph or certain text) and the collection of metadata is of lesser importance.[127]

b. Self-Collection Based on Social Media Processes

Various social media platforms have established means by which a user can download social media data. Platforms also have procedures for carrying out a download, which differ in the form and appearance of data that they provide to the subscriber.

Facebook, for example, requires a username and password to process a download request, and as a result, this process must generally be carried out by the account user (or someone to whom the user has provided login credentials).[128] The download includes various categories of information, including advertisements on which the user has clicked and communications exchanged on Facebook Messenger. It is provided in HyperText Markup Language (HTML) plain text files. Although the information from the Facebook download can perhaps be used as evidence in particular situations, it may be preferable to have a vendor obtain the data with the appropriate tools for accessing and then reviewing the information in a manner that includes available metadata.

Twitter offers a "request your archive" service. This request goes to Twitter, which provides the user with a download link

127. For example, Snapchat conversations disappear as soon as they are read unless a screenshot is taken as recognized in *R v White-Halliwell*, 2019 ONSC 597 at paras 70–72.

128. See *How do I download a copy of my information on Facebook*, online: Facebook Help Ctr. < https://www.facebook.com/help/212802592074644?elpref=related > (last visited 15 Sept. 2021).

to a ZIP file sent to the confirmed account email address.[129] This download gives the user copies of all the user's tweets since the account's creation.

LinkedIn offers a download option from the user's account. The process involves two steps: first, using the privacy settings to request an archive of the user's data, which provides within minutes the ability to download information regarding messages, connections, and contacts. Within 24 hours, LinkedIn provides an email link that allows the user to obtain a full archive of the user's data, including activity and account history.[130]

WhatsApp facilitates conversation history exports from within the application itself. These exports generate a plain-text version of the text communication; however, exports are limited to a maximum number of messages and media (i.e., images and video files) before and after those currently displayed on the phone's screen.[131] These exports, while easy to perform, may not capture the entirety of the conversation, and the generated plain-text file is easy to modify after export.

Reliance on provider-controlled export tools, such as those described above, may raise preservation and collection issues. These tools are often modified or updated by the service provider, without necessarily making the user aware of those

---

129. *How to Download Your Twitter Archive,* online: Twitter Help Ctr., <https://help.twitter.com/en/managing-your-account/how-to-download-your-twitter-archive> (last visited 15 Sept. 2021).

130. *Accessing Your Account Data,* online: LinkedIn Help <https://www.linkedin.com/help/linkedin/answer/50191/accessing-your-account-data?lang=en> (last visited 15 Sept. 2021).

131. As of August 2020, the export feature is limited to 40,000 messages when exported without media, or 10,000 messages and a selection of most recent images. *How to save your chat history*, online: WhatsApp <https://faq.whatsapp.com/android/chats/how-to-save-your-chat-history/> (last visited 15 Sept. 2021).

changes. For example, Facebook's tool may cap the number of Messenger messages exported, potentially omitting responsive messages from the exported data. Although self-collection may be an easier option for some subscribers as a means of preservation, the frequent changes to the export tools pose some risk that counsel should consider.

c. Use of an Application Programming Interface Offered by the Social Media Provider

Several social media providers have created utilities that allow third parties to access the social media provider's application and exchange information with that application. These utilities, using an Application Programming Interface (API), allow eDiscovery vendors to access the social media platform and import selected data in a machine-readable format that captures both content and various metadata associated with the content.

Vendors may capture individual items on the platform with metadata attached in a manner that permits search and review of the content. These tools collect metadata that can help with corroboration and potential authentication of the underlying content and may generate a message-digest hash for verification of the extracted data.[132]

Facebook, Twitter, Flickr, and Tumblr, among others, have APIs that allow access to their web content. These APIs all have different operating formats, but vendors have developed their own programs to download the data made available by the

132. For example, a "tweet" generated on Twitter or an individual Facebook post contains over 20 specific metadata items. See John Patzakis, *Key Facebook Metadata Fields Lawyers and eDiscovery Professionals Need to be Aware of* (11 Oct. 2011), online: eDiscovery L. & Tech Blog <http://blog.x1discovery.com/2011/10/11/key-facebook-metadata-fields-lawyers-and-ediscovery-professionals-need-to-be-aware-of>.

social media provider's API.[133] Among messaging applications, Slack also has an API that may allow access to vendors.[134]

Social media providers set the standards on web content that may be downloaded. In 2015, Facebook changed its prior policy of giving access through its API to almost all public-facing information to a more restrictive policy that does not permit collection of data on user timelines or personal profiles, and allows access only to public pages that could be liked or followed.[135] Twitter provides information through its API on individual users and their tweets.[136]

The API process cannot produce a forensic image of the captured web content because it changes and transforms the original context and format of the underlying content. There is also a chance that the content will not be rendered in an identical manner to the way it appeared on the service provider's site. Despite these issues, content produced using a social media

---

133. One of the popular social media discovery collection tools is X1 Social Discovery, which has API collection tools for Facebook, Twitter, YouTube, Instagram, and Tumblr, along with the capability to collect webpages and email from other providers. See *Collect and Search Data From Social Networks and the Internet*, online: X1 <https://www.x1.com/products/x1-social-discovery/> (last visited 15 Sept. 2021).

134. See, *e.g., Guide to Slack import and export tools,* online: Slack Help Ctr. <https://get.slack.help/hc/en-us/articles/204897248-Guide-to-Slack-import-and-export-tools> (last visited 7 June 2021).

135. See *Terms of Service,* online: Facebook <https://www.facebook.com/terms.php?ref=p> (last visited 8 March 2021); see also *What Type of Web Data Can You Collect From Facebook?* (17 June 2016), online: Bright Planet <https://brightplanet.com/2016/06/type-web-data-can-collect-facebook/>.

136. See *Twitter Terms of Service,* online: Twitter <https://twitter.com/en/tos> (last visited 8 March 82021); see also *What Type of Data Can You Get from Twitter* (15 March 2016), online: Bright Planet <https://brightplanet.com/2016/03/what-type-of-data-you-can-get-from-twitter/>.

provider's API has routinely been admitted into evidence at trial and is considered a best practice.

d. Original Digital Format or Near-Original Digital Format of the Web Content

With the International Organization for Standardization (ISO) 28500 Web ARChive (WARC) standard, it is possible to get an original digital format or near-original digital format file of the collected content of a social media platform. This standard, established by the International Internet Preservation Consortium, uses a WARC file as a container or image for accessed web resources and metadata.[137] A web crawler or similar program captures the data, stores the data in a WARC file, and generates relevant metadata about the capture to confirm that the data has been obtained and that its integrity has been preserved. The captured data has working links, graphics, and other dynamic content, along with an audit trail tracing back to the original social media platform.

With the original digital format or near-original digital format file capture, the data can be viewed as the content originally appeared on the social media platform, although it may not be possible to view all of the linked content. The data can be searched, reviewed for metadata, and exported to an eDiscovery platform for further review.

To carry out this imaging of the web content, it would be necessary to have the consent of the user.

137. *ISO 28500:2017 Information and documentation—WARC file format*, online: ISO <https://www.iso.org/standard/68004.html> (last visited 8 March 2021).

e. Other Vendor Services, Including Dynamic Capture

Vendors have developed technology to allow certain content to be collected in a way that preserves the content and captures various metadata fields associated with social media data. Properly captured, these metadata fields can assist with establishing the chain of custody and authentication. They can also help to facilitate more accurate and efficient data processing and review.

Dynamic capture can assist with the preservation and collection of social media. This process captures and analyzes the resulting digital materials based on specific business rules. This analysis allows a party to draw conclusions about the data set based on the rules applied to the data, without corrupting the data.

In litigation, dynamic capture processes can be applied to interactive content in cloud-based collaboration sites that needs to be preserved and reviewed. It may also apply to situations involving large amounts of user data on a social media platform. Dynamic capture allows a vendor to identify relevant data in the collaboration site or capture interactive data on the social media platform. It then creates data sets that can be reviewed and searched to identify relevant data for litigation without altering it.

Technology to preserve, collect, and review social media continues to adapt to new services and social media offerings. Similar to early generation email review, where slow and relatively simple technologies were rapidly supplanted by a variety of sophisticated email review options, eDiscovery tools addressing social media will undoubtedly grow in capacity and capabilities and should in the future be able to handle more of the challenges that social media poses.

D. Review and Production

1. Review

The way in which social media data will generally be reviewed for discovery purposes is driven by how the data was preserved and collected and by what is feasible under the circumstances. Selecting the proper approach for review may involve several factors, including whether there is a need to review the data interactively as it appeared on the social media platform or to see how the content changed over time. Other factors may include the volume of the data to be reviewed, whether metadata was collected and is relevant, and the ability of the review software to facilitate coding and to support litigation processing and management needs. Those needs may include, among other things, search, sampling, Bates stamping, redaction, and export. A final factor is whether to allow the requesting party to inspect and copy relevant content from the social media accounts at issue.[138]

---

138. *Rules of Civil Procedure*, RRO 1990, O Reg 194, r 30.04; *Alberta Rules of Court*, Alta Reg 124/2010, s.5.14; *Supreme Court Civil Rules*, BC Reg 168/2009, r 7-1(15); *Court of Queen's Bench Rules*, Man Reg 553/88, r 30.04; *Rules of Court*, NB Reg 82-73, r 31.04; *Rules of the Supreme Court*, SNL 1986 c 42, Sch. D, r 32.05; *Rules of the Supreme Court of the Northwest Territories*, NWT Reg 010-96, s.225; *Rules of the Supreme Court of the Northwest Territories*, NWT Reg 010-96 (Nu), s.225; *Nova Scotia Civil Procedure Rules,* Royal Gazette Nov 19, 2008 at rr 16.05-16.06; *Supreme Court Rules of Civil Procedure*, Prince Edward Island, r 30.04; *The Queen's Bench Rules*, Sask. Gaz. December 27, 2013, 2684, Part 5-11; *Rules of Court*, YOIC 2009/65, r 25(4); *Tax Court of Canada Rules (General Procedure)*, SOR/90-688a, r 85; and *Federal Courts Rules,* SOR/98-106, r 228. See *Marineland of Canada Inc. v. Demers*, 2017 ONSC 2230 (defendant not required to produce a hard copy of records if publicly available after listing relevant websites in Schedule A of his affidavit of documents); *Schuster v. Royal & Sun Alliance Insurance Company of Canada*, 2009 CanLII 58971 (ON SC) at paras 17–18 (it is beyond the scope of discovery obligations to produce user name and passwords for social medial accounts). FED. R. CIV. P. 34(a). Such a course

a. Small Data Volumes

It may be preferable to review social media content using the original digital format or near-original digital format file or the API used for collection when the data volume is small. These methods are also useful if a responding party needs to review the social media data interactively, as it was originally displayed on the platform, or over a certain period of time. Available social media and API products can be used to collect an entire archive or certain categories of information associated with the social media account, such as chat messages, account activity, and multimedia files, making the review experience similar to the experience the user had when uploading or posting content. This functionality could be important in a trademark case, for example, where the way the allegedly infringing mark is displayed throughout a platform and over time is critical.

Parties might alternatively consider obtaining archival downloads of user information from social media accounts, although such downloads have their limitations. With Facebook and Twitter, users may only download the entirety of their accounts and cannot limit the download to relevant content. In addition, an archival download may not include all relevant

may be preferable for some parties who might consider a review to be unduly burdensome. See *McDonald v. Escape the Room Experience*, LLC, No. 15-cv-7101 RAK NF, 2016 WL 5793992, at *1 (S.D.N.Y. Sept. 21, 2016) (rejecting plaintiff's argument that it would be "unduly burdensome" to produce her Facebook postings).

data.[139] Information may also be difficult to review.[140] Moreover, the content and format of provider-created archives may be periodically changed or updated by the service provider, rendering the archives unreliable for preservation purposes.

b. Large Data Volumes

When large volumes of social media data are involved, it may be preferable to use early case assessment and review tools to filter the content and accomplish the review. Selecting a review tool for social media may be particularly useful when the case team is most concerned with the text from social media platforms as opposed to the way data was originally displayed. Reviewing social media content in a review tool is also practical when the content was preserved and collected in a manner that rendered it more like other types of ESI, enabling reviewers to use features such as threading and bulk tagging.

Data clustering and near duplicate identification technologies may also be helpful in identifying content from social media data that is similar to and can be grouped with other ESI such as email and loose files. Extended social media communication often takes place over several different types of media.

---

139. Archived information may not provide context surrounding certain user comments. More sophisticated tools may be required to capture a snapshot in time of the social media interface on which comments were made. In addition, the Twitter archive does not include messages exchanged with other users through the platform messaging interface. In one case, a court ordered production of a family computer hard drive to help determine an individual's Facebook usage activity: *Bishop (Litigation Guardian of) v. Minichiello*, 2009 BCSC 358 (B.C. S.C.), leave to appeal B.C.C.A. ref'd 2009 BCCA 555.

140. Posts and photos in a Facebook archive download into different folders, and the posting list renders as a crudely formatted list in hypertext markup language (HTML) file. Tweets download to a comma separated value (CSV) file format in Excel.

For example, such a communication may begin with messaging, move to phone, then to text, and end with video. Technology that allows these different forms of communication—all residing in different services and saved in different file types—to be reviewed together can be useful for understanding the full context and content of such communication. Such capability also prevents social media data from being reviewed in isolation. This functionality is optimized when social media metadata is available.

If the social media content is loaded into a review platform, it will be important to consider how the content will be organized as "documents" within the platform. A "document," for instance, could reflect a page, a site, a user homepage, an email, a blog post, or a picture. Content may need to be parsed and reconstructed to make it manageable for review as well as to give context.

Despite the benefits of review platforms, they are generally not programmed to mimic the interactive experience of a social media platform. The difficulty in collecting metadata associated with the social media content, combined with other issues such as the tendency of social media postings to incorporate content from external sites, can make using a conventional platform to review social media content difficult or inefficient. As with the ongoing work surrounding the collection of social media content, review platforms are also rapidly evolving to display social media in more intuitive and appropriate formats.

2. Production

The same analysis that guides the selection of an appropriate review platform also applies to the production of social media

data.[141] The issue turns on the importance to the case for the requesting party to be able to review the social media data interactively and as it appeared on the social media platform. When interactive review is not important, it may be sufficient to produce the social media content in a reasonably usable and searchable format with or without metadata. Where messaging, texts, or similar text-based content are the primary data being produced, they can usually be handled in the same manner as traditional text-based content such as email.

In cases involving small amounts of social media data, static images or hard-copy printouts are often used for review and production.[142] Doing so, however, may run afoul of the requesting party's production requests or a desire to produce in a reasonably usable format.[143] The complexities surrounding social media production emphasize the need for dialogue and cooperation between requesting and responding parties.

It will sometimes be important to produce the relevant social media data in an interactive format that imitates the way it

---

141. Definitions of "document" are found at the following sections in the respective province's rules: *Ontario Rules*, *supra* note 11515, r 30.01; *BC Rules*, *supra* note 115, r 1; *Manitoba Rules*, *supra* note 115, r. 30.01; *NB Rules*, *supra* note 11515, r 31.01; *NWT Rules*, *supra* note 11515, r 218; *Nu Rules*, *supra* note 11515, r 218; *Yukon Rules*, *supra* note 11515, r 1 (8); *PEI Rules*, *supra* note 11515, r 30.01; *Saskatchewan Rules*, Part 17; *Québec, An Act to establish a legal framework for information technology*, RSQ c C-1.1 [*Québec Information Technology Act*], s 3; *Tax Court Rules*, *supra* note 11515, r 78; *Federal Courts Rules*, *supra* note 11515, r 222(1).

142. See, *e.g.*, *J.C. v. M.C.,* 2014 NBQB 161 at para 9 (party produced hard copy of a text message conversation at the request of the court).

143. See *Cholakis v. Cholakis* (2000), 44 C.P.C. (4th) 162 (M.B.Q.B.) (Court ordered production of accounting data in electronic format even though it had already been produced on paper); *Walter Construction (Canada) Ltd. v. Greater Vancouver Sewerage and Drainage District*, 2003 BCSC 1582 (electronic documents ordered to be produced despite documents already being provided in hard copy).

appeared on the platform. Production in this manner would be consistent with the concept that a reasonably usable production format is typically one that allows the receiving party to make use of data in the same or similar way as the responding party ordinarily maintained the content.

There are different potential responses to this request. One strategy is to give the requesting party access to a copy of the original digital format or near-original digital format file or to certain portions of the API used for collection. Another strategy is for the responding party to produce static images of the pertinent platforms so the requesting party may observe how they appeared. While unlikely to be required to do so by a court, the responding party may choose to grant the requesting party access to the social media account in order to review the content interactively.[144] Providing adversaries with direct access to a responding party's social media account should be a last resort, if done at all, e.g., when there is no other way to accomplish production and when it is critical that opponents have interactive and similar use of the content.[145] A responding party exercising this option should consider potential safeguards to be implemented, such as a written agreement with the reviewing party restricting what information can be accessed and reviewed, only permitting access under supervision and only for a limited period of time, and either not sharing login details or immediately changing them after access.

Depending on whether the cost is proportional to the needs of the case, engaging a neutral vendor may be helpful to assist with challenges in social media production. In one U.S. case, a

144. Courts have held it is beyond the scope of discovery obligations to force a party to produce social medial passwords: *Schuster v. Royal & Sun Alliance Insurance Company of Canada*, 2009 CanLII 58971 (ON SC) at paras 17–18.

145. See *supra* Section III(D)(8).

vendor collected the defendant's devices, and the defendant granted the vendor access to his social media accounts, which contained millions of pages of data. The vendor then ran search terms agreed to by the parties and provided only responsive material to the plaintiff.[146]

146. *Pre-Paid Legal Servs., Inc. v. Cahill*, No. 6:2012-cv-0346, 2016 WL 8673142, at *1 (Sept. 30, 2016). For a more common alternative, see *Loblaws Inc. v. Columbia Insurance Co.*, 2019 FC 961 at para 152 (expert using keyword searches of social media accounts to find relevant posts).

IV. CROSS-BORDER DISCOVERY ISSUES

Parties who seek discovery of information from persons outside of Canada or social media information located in a foreign country should determine whether there are laws that preclude the processing, transfer, or production of social media information. Parties seeking social media information within Canada may consult federal laws focused on the protection of personal data in commercial activities.[147] Personal data may also be protected more broadly by treaty[148] or applicable foreign law outside of Canadian borders.

A. United States

The U.S. lacks comprehensive, centralized data protection laws. Recently, states such as California, Nevada, and Maine

147. Federally, the Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) (PIPEDA) applies to data collection, use and disclosure of personal information by private sector conducting commercial activities across Canada, and employment information of federally regulated organizations. All businesses that operate within Canada and handle personal information that crosses provincial or national borders are subject to PIPEDA. For more information, see *supra* Section III.A.1, "Privacy Obligations."

148. *Charter of Fundamental Rights of the European Union* (EU), 2000 O.J. (C 364) 1, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1544731399799&uri=CELEX:32000X1218(01)> [hereinafter Charter of European Union]. In addition, the African Union Convention on Cyber Security and Personal Data was adopted on June 27, 2014 and requires the creation of an independent administrative authority tasked with protecting personal data. However, as of June 2020, out of 55 countries, only five (Ghana, Guinea, Mauritius, Namibia, Senegal) have ratified the treaty. See *African Union Convention on Cyber Security and Personal Data Protection*, June 27, 2014, EX.CL/846(XXV), online: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>.

have enacted privacy legislation.[149] More broadly, the U.S. is party to the Hague Convention of the Taking of Evidence Abroad in Civil or Commercial Matters (Hague Evidence Convention). The Hague Evidence Convention allows authorities in one signatory country to obtain evidence located in another signatory country within judicial proceedings by means of a Letter of Request. While Canada is not a signatory to the Hague Evidence Convention, the U.S. has codified the Hague Convention within 28 U.S. Code § 1782. Canadian parties seeking evidence from the U.S. can still achieve this process by securing letters of request or letters rogatory from a Canadian court and applying to a U.S. court for enforcement through Section 1782.

B. Europe

While Canada is not a signatory to the Hague Evidence Convention, it has entered into bilateral treaties with a number of EU member states for judicial cooperation when requesting evidence abroad.[150]

The European Union (EU) provides broad protections of personally identifiable information. Defined broadly, "personal data" includes any information relating to an identifiable individual.[151] Like Canada, the EU views the privacy of "personal

---

149. *California Consumer Privacy Act*, Cal. Civ. Code §1798.100 (West 2018), online: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5>, *An Act to Protect the Privacy of Online Consumer Information*, Me. Rev. Stat. Ann. . § 9301 (2019) online: <https://www.mainelegislature.org/legis/bills/bills_129th/billtexts/SP027501.asp>; Nev. Rev. Stat. § 603A (2019) online: <https://www.leg.state.nv.us/NRS/NRS-603A.html>.

150. *Response Canada to 2008 Evidence Questionnaire*, online: <https://assets.hcch.net/upload/wop/2008canada20e.pdf>.

151. 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

data" as a "fundamental human right."[152] An even stricter standard of protection applies to sensitive personal information such as racial or ethnic origin, religious beliefs, and political opinions.[153]

The General Data Protection Regulation (GDPR) is the basis of EU data protection law. The GDPR allows for data transfers to countries like Canada, whose legal regime was found by the Commission to provide an "adequate" level of personal data protection.[154]

The GDPR broadly defines the "processing" of data and proscribes the processing of personal data unless an exception applies. Processing includes "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[155] A party's actions in preserving or collecting social media content will likely be considered

---

repealing Directive 95/46/EC, 2016 O.J. (L119) 1, at art. 4(1) [GDPR], online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN> (prohibiting the processing of such personal information barring narrow, delineated exceptions).

152. *Charter of European Union*, *supra* note 148, at art. 8; Section 8 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, s 91(24).

153. *GDPR*, *supra* note 151, at art. 9.

154. *Ibid* at art. 45; Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539) (2002/2/EC) at art 1, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02002D0002-20161217&from=EN>.

155. *Ibid* at art. 2.

"processing." Unless an exception such as consent (obtained from a data subject) applies or where processing is "necessary for compliance with a legal obligation to which the controller is subject,"[156] such processing could violate the GDPR.

While the GDPR applies to all member states, there are several provisions that allow member states to independently interpret domestic data protection legislation.[157] Canadian parties looking to control and process personal information from the EU should consult specific member state legislation in addition to the GDPR to determine whether additional steps are required to maintain compliance.

C. Asia

Canada is a founding member of the Asia-Pacific Economic Cooperation (APEC) and a member of APEC's Cross-Border Privacy Rules System (CBPR). The APEC Privacy Framework sets out nine guiding principles related to privacy.[158] Similar to both Canada and the EU, the APEC Privacy Framework takes a broad view of privacy and employs stringent protections. CBPR establishes a privacy framework for the transfer of personal data by participating countries.[159] Parties seeking cross-border discovery of social media must satisfy the CBPR or otherwise reach an acceptable data transfer agreement that provides for the protection of personal data.

A more thorough analysis of treaties, laws, and regulations affecting cross-border discovery of social media is beyond the

---

156. *Ibid* at art. 6.

157. For example, i*bid* at art. 6(2).

158. See *APEC Privacy Framework* (2015), online: Asia-Pacific Economic Cooperation <https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)>.

159. *Cross Border Privacy Rules System*, online: <http://www.cbprs.org/> (last visited June 21, 2020).

scope of the *Sedona Canada Commentary on Discovery of Social Media*. The Sedona Conference's *Practical In-House Approaches for Cross-Border Discovery & Data Protection*[160] and *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*[161] provide additional information, as well as guidance and best practices regarding the interplay between cross-border laws and regulations and the U.S. discovery process.

160. 17 Sedona Conf. J. 397 (2016).

161. See The Sedona Conference, "International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)" (January 2017), online: <https://thesedonaconference.org/publication/International_Litigation_Principles>.

V. AUTHENTICATION OF SOCIAL MEDIA EVIDENCE

The Canada Evidence Act[162] (CEA) and most provincial evidence statues contain provisions that relate to the admissibility of "electronic evidence." As will be seen below, these provisions only concern authentication and the application of the best evidence rule as they relate to electronic evidence. They do not affect any rule of law relating to the admissibility of evidence.[163] While the evidence statutes' requirements are mandatory,[164] the ultimate admissibility of the evidence depends on the purpose for which it is tendered and any related general law of evidence. Failure to attend to the evidence statutes' requirements has resulted in evidence ruled inadmissible even though the requirements would have been easily met.[165]

Subsections 31.1 to 31.8 of the CEA apply to "electronic documents," which are defined as: "data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data."[166] This broad definition would include copies of any documents stored in a computer or smartphone, including social media evidence such as Facebook posts, emails, and other forms of electronic communications.[167]

---

162. *Canada Evidence Act*, R.S.C. 1985, c. C-5.

163. *Ibid*, s. 31.7.

164. *Richardson v. R.*, 2020 NBCA 35 at para 32.

165. *R. v. Donaldson*, 2016 CarswellOnt 21760, [2016] O.J. No. 7153, 140 W.C.B. (2d) 513, at paras 3–4 and 22. See also *R. v. Ball* 2019 BCCA 32 at para 86 and *R. v. Bernard* 2016 NSSC 358 at para 40.

166. Canada Evidence Act, supra note 162, s. 31.8.

167. *R. v. Ball*, 2019 BCCA 32 at para 67; *Richardson v. R.*, 2020 NBCA 35 at para 22.

The provisions of the Canada Evidence Act that concern electronic documents modify the common law rules of authenticity and "best evidence" to address the unique nature of electronic evidence.[168]

A. Authentication

The most fundamental rule governing the admissibility of any form of documentary evidence is that the document must be authenticated.[169] This requires the person proffering an item into evidence to give evidence that the item is what it purports to be. At common law, this requirement was met by providing "some evidence" to establish that fact. It is a low standard that can be met by either direct or circumstantial evidence.[170]

Section 31.1 of the CEA codifies the authenticity requirement. It provides that the person "seeking to admit an electronic document has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is what it is purported to be." The Court of Appeal for Ontario has interpreted the words "evidence capable of supporting" as evidencing a low threshold.[171] It is important to keep in mind that under this low threshold, a document may be authenticated even though there are competing claims as to the document's "genuineness." In other words, if the party offering the document into evidence provides evidence capable of supporting that it is genuine, the test will be met regardless of the strength of the contrary view. This is because disputes about authenticity are better resolved at the end of the case with an

168. *R. v. Avanes et al.*, 2015 ONCJ 606 at para 55.

169. McWilliams' Canadian Criminal Evidence, 5th ed, 24:40:10.

170. *R. v. C.B.*, 2019 ONCA 380, at para 66.

171. *R. v. S.H.* 2019 ONCA 669 at para 25.

appreciation of all the evidence.[172] The integrity or reliability of the electronic document is not open to attack at the authentication stage of the enquiry.[173]

Section 31.1 does not limit how and by what means authenticity may be established.[174] The test would be met if witness presented with an electronic document was able to articulate some basis for authenticating it as what it purports to be. In *R. v. K.M.*,[175] for example, the Court held that the authentication requirement had been met when a witness testified that a printout of Facebook messages exchanged with the accused "reflected what he could see on the computer screen [. . .] after logging on to his Facebook account."[176]

The authenticity requirement may also be met by providing circumstantial evidence that the document is what it purports to be. For example, in a case where the police seized password-protected Blackberries, which required specialized expertise to extract their contents, the Ontario Court of Justice held that the authenticity requirement had been met when the PIN numbers on the extracted messages matched the PIN numbers on the Blackberries themselves.[177]

Another useful manner of meeting the authenticity requirement through circumstantial evidence is through the common law "reply letter" doctrine. It holds that correspondence can be authenticated as having been sent by an individual by showing

---

172. David M. Paciocco, "Proof and Progress: Coping with the Law of Evidence in a Technological Age" (2013) 11 C.J.L.T. 181 at 197.

173. *R. v. Hirsch*, 2017 SKCA 14 at para 18.

174. *R. v. C.B.*, 2019 ONCA 380, at para 68; *R. v. Hirsch*, 2017 SKCA 14 at para 18.

175. 2016 NWTSC 36.

176. *Ibid*, at paras 16 and 36.

177. *R. v. Arvanes et al*, 2015 ONCJ 606 at paras 66–68.

that it is a reply to a letter sent to that individual.[178] As a matter of logic, the same should hold true for text messages and emails. If a person sent a text or email to the email address or phone number believed to be linked with the intended recipient, evidence of a response purportedly from that person affords some evidence of authenticity.[179]

B. "Best Evidence" Requirement

At common law, the best evidence rule required a party to produce the best evidence available. The rule sought to avoid fraud or forgery[180] and is premised on the notion that forgery would be easier to detect on an original document than on a copy.[181] This rule has declined in importance, and its remnants in Canada states that "if an original document is available in one's hands, one must produce it."[182] The concept of an original is not readily applied to electronic documents.[183] However, the Canada Evidence Act's broad definition of "electronic document" embraces any data that is translated from computer code and can be read or perceived, including a display or printout.

Most provinces have passed legislation that provides guidance for the use of electronic means for creating and managing records.[184] Currently, legislation across Canada provides a

178. Paciocco, *supra* note 172, at 197.

179. *R. v. C.B.*, 2019 ONCA 380, at para 68.

180. R. v. After Dark Enterprises Ltd., (1994) ABCA 360 at para 9.

181. *R. v. Sampson,* 2020 BCPC 27 at para 23.

182. Paciocco, *supra* note 172, at 199.

183. *R. v. Hirsch,* 2017 SKCA 14 at para 22.

184. The Yukon, Prince Edward Island, Ontario, Newfoundland, Nova Scotia, and Nunavut have respectively passed: *Electronic Commerce Act*, RSY 2002, c 66; RSPEI 1988, c E-4.1; SO 2000, c 17; SNL 2001, c.E-5.2; SNS 2000, c 26; and SNu 2004, c 7. Alberta, New Brunswick, British Columbia, and the North West Territories have similar legislation under the title of the *Electronic*

means to facilitate the admissibility of ESI in the courts, including the establishment of evidentiary presumptions related to integrity of electronic information and procedures for introducing such evidence and challenging its admissibility, accuracy, and integrity. The legislation generally does not modify any common law or statutory rule related to the admissibility of records, except the rules relating to authentication and best evidence.[185] Section 31.2 of the Canada Evidence Act provides four different ways of satisfying the best evidence rule. As will be seen below, these "best evidence" provisions provide assurance that "the document provided to the Court is the same as the one that was input into the computer" and are therefore an "adjunct to authenticity."[186] Each of the statutory conditions described below may be proven by calling a witness or by filing an affidavit under subsection 31.6.

1. Proving the integrity of the system that recorded or stored the document

Subsection 31.2(1)(a) provides that the best evidence rule is satisfied on proof of the integrity of the electronic document system by or in which the electronic document was recorded or stored. The standard of proof is on the balance of probabilities

---

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: *Québec Information Technology Act*, *supra* note 14141.

185. *See, e.g.*, *Evidence Act*, RSO 1990 c E.23, s 34.1 [*Ontario Evidence Act*]; *Québec Information Technology Act*, *supra* note 14141, s 5, 6 and 7.

186. Paciocco, *supra* note 172, at 200; see also *Richardson v. R.*, 2020 NBCA 35 at para 28.

and requires the party seeking admission to establish that it is more probable than not that the system had integrity.[187]

Proving that the system had integrity requires one to establish that the electronic document system had the capacity to accurately record, maintain, and display the data.[188] This can be established through direct evidence about the operation of the system. For example, the Court was satisfied that a computer system had integrity and admitted Facebook messages when one of the parties testified about the steps she took to engage in a chat and testifying that the system worked in the usual way.[189] If the opposing party admits to have authored postings on social media platforms that are at issue, integrity of the computer system will have been proved.[190]

2. Proving the integrity of the system though one of the presumptions of integrity

A party may rely on one of the presumptions contained in subsection 31.3 to prove the integrity of the computer system. Different standards of proof apply to the various presumptions described below:

> c. By providing evidence capable of proving that the system was operating properly, or if it was not, that it did not affect the integrity of the documents

Subsection 31.3(a) sets a low threshold of proof by merely requiring "evidence capable of supporting a finding" that the

187. Paciocco, *supra* note 172, at 202; *see also Richardson v. R.*, 2020 NBCA 35 at para 32.

188. Paciocco, *supra* note 172, at 202.

189. *R. v. Soh*, 2014 NBBR20 at paras 28–30.

190. *Holden v. Hanlon*, 2019 BCSC 622 at para 50.

computer system was operating properly.[191] The evidence can be direct or circumstantial. Evidence that an email was received on a device such as a computer or a phone and that it was readable and coherent would meet this requirement.[192] The Court of Appeal for Ontario held that the text messages extracted from a person's smartphone that were in "chronological order and customary format, demonstrating coherent conversations between a sender and a recipient" could support a finding that the smartphone was working properly.[193] The fact that the content of the text messages is congruent with other evidence at trial can also support a finding that the device is working properly.[194]

d. By establishing that the electronic document was recorded or stored by an adverse party.

Subsection 31.3(b) provides that the integrity of the system that stored or recorded an electronic document may be proved by establishing that the document was recorded or stored by an adverse party. The fact underlying this presumption (the document was stored or recorded by an adverse party) must be proved on the balance of probabilities. This presumption is based on the notion that the opposing party who stored or recorded the document is in the best position to explain if the computer system was unreliable.

191. *Canada Evidence Act*, *supra* note 162, ss. 31.3(a); *R. v. S.H.* 2019 ONCA 669 at para 25.

192. Paciocco, *supra* note 172, at 202.

193. *R. v. S.H.* 2019 ONCA 669 at paras 24–27.

194. *Ibid* at para 27.

e. Presumption of integrity if the electronic document is a business record

Subsection 31.3(c) provides that the system that stored or recorded the electronic document has integrity if it is established that the document was recorded or stored in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce the document.[195] This presumption could be used where an internet service provider produces text messages as a result of a production order. Duplicate receipts stored in a pharmacists' computer were found to meet this presumption.[196]

3. Presumption of integrity based on electronic signature

Section 31.4 provides that regulations may be made establishing evidentiary presumption in relation to secure electronic signatures. The Secure Electronic Signature Regulations[197] establish such a presumption. A document signed with a "secure electronic signature" (meeting certain defined technical requirements) will be presumed to have been signed by the person identified in the digital signature certificate.[198]

4. Printouts that have been manifestly and consistently relied upon

The final method of meeting the best evidence requirement is the presumption, contained in section 31.2(2), that applies to printouts that have been "manifestly and consistently acted on,

195. *Canada Evidence Act*, *supra* note 162, ss. 31.3(c).

196. *R. v. Piercey*, 2012 ONCJ 500 at paras 26–27.

197. SOR/ 2005-30.

198. *Ibid* at s. 5.

relied on or used as a record or the information recorded or stored in the printout."

VI. ETHICAL ISSUES RELATED TO SOCIAL MEDIA AS POTENTIAL EVIDENCE

Social media discovery implicates various ethics rules for counsel. These rules involve the preservation and production of such information and the equally significant issue of counsel's use of social media.

A. Counsel Duty of Technology Competence

The Federation of Law Societies of Canada's Model Code of Professional Conduct ("The Code") require lawyers to understand the impact and consequences of technology use by clients and counsel. The Model's duty of technology competence requires that lawyers develop an understanding of, and ability to use, technology relevant to the nature and area of the lawyer's practice and responsibilities.[199] The Code sets out statements of principle followed by exemplary rules and commentaries. The Code is a model that the individual provinces and territories may or may not incorporate into their own codes.

B. Counsel's Use of Social Media for Discovery

Counsel must remember the rules of professional conduct when seeking social media content through informal methods or through the formal discovery process. Either scenario can present ethical traps.

Counsel may informally seek messages, posts, or other social media content, as the rules of professional conduct do not impose a blanket prohibition on such discovery. This occurs when social media content is available on platforms, applications, or the internet without restrictions. In contrast, when relevant

199. The Federation of Law Societies of Canada, *Model Code of Professional Conduct*, as amended 19 October 2019, online: <https://flsc.ca/wp-content/uploads/2019/11/Model-Code-October-2019.pdf>.

content is not readily available without obtaining formal permission from the social media user, ethical violations can occur. These ethical violations could come in the form of impersonation or pretext when attempting to gain access to information that is not publicly available (for example, by "friending" a party's social media account). A quintessential example of this type of professional misconduct occurs when counsel seeks a connection on social media with a person who is or may become a party, witness, or juror in a lawsuit. If there is any doubt regarding the propriety of counsel's method for seeking social media evidence, the more prudent course is to use the formal discovery process.

Formal discovery does not eliminate the potential for ethical challenges. Social media accounts are often a dossier of private or sensitive information, including correspondence with intimates, notations that are the equivalent of journal entries, and photographs. Discovery requests that demand the entirety of a person's social media account without reasonable limitations on time or scope may be considered harassing, burdensome, or otherwise improper. Such "frivolous" requests may thus violate the principle of proportionality and could also be grounds for discovery sanctions.[200]

200. Law Society of Ontario, *Rules of professional conduct*, rule 5.1-3.1(c); Law society of Prince Edward Island, C*ode of professional conduct*, rule 5.1-3.1(c) ("a lawyer, when acting as an advocate . . . (c) shall not make frivolous requests for the production of documents or make frivolous demands for information at the examination for discovery."). Other rules of professional contain broader statements suggesting counsel avoid and discourage resort to frivolous or vexatious behaviour.

VII. CONCLUSION

While the *Sedona Canada Commentary on Discovery of Social Media* offers insightful guidance on social media discovery issues as they stand in 2021, social media will almost certainly remain a dynamic area for technological development. As innovations continue to change the social media landscape, court decisions and other laws will likely advance to address new technological challenges. Counsel should therefore stay abreast of ongoing technological and legal developments to ensure continued understanding of the issues surrounding discovery of social media.

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

This publication may be cited as follows:

> The Sedona Conference, *The Sedona Canada Principles Addressing Electronic Discovery*, 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*, RSPEl 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).

THE SEDONA CONFERENCE PRIMER ON CRAFTING EDISCOVERY REQUESTS WITH "REASONABLE PARTICULARITY"

A Project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)

Author:

The Sedona Conference

Drafting Team Leaders:

Rebekah L. Bailey
Donald W. Myers

Drafting Team:

Scott J. Borrowman
Kelly M. Cullen
MaryBeth V. Gibson
Jill C. Griset
Greg Kohn
Kristen Orr
J. Michael Showalter

Judicial Observer:

The Hon. Kristen L. Mix

Steering Committee Liaisons

Lea Melani Bays
Jennifer S. Coleman
Greg Kohn
Lauren Schwartzreich

Staff editor:

David Lumia

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

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, *Primer on Crafting eDiscovery Requests with "Reasonable Particularity,"* 23 SEDONA CONF. J. 331 (2022).

PREFACE

Welcome to the final, January 2022 version of The Sedona Conference *Primer on Crafting eDiscovery Requests with "Reasonable Particularity" ("Primer")*, a project of The Sedona Conference Working Group 1 on Electronic Document Retention and Production (WG1). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

In March 2018, WG1 published the *Federal Rule of Civil Procedure 34(b)(2) Primer*, providing practical pointers on responding to discovery requests and a detailed framework for drafting responses to requests for production that comply with amended Rule 34(b)(2). However, the *Rule 34(b)(2) Primer* did not address one of the causes of poorly drafted Rule 34 responses: Deficiencies with Rule 34 *requests*. Vague and overbroad discovery requests continue to clog the courts and increase litigation costs. This *Primer* is intended to provide practical considerations for drafting requests for production in compliance with Rule 34(b)(1). It's hoped that the guidance in this *Primer*, along with the *Rule 34(b)(2) Primer*, will result in more efficient discovery, reduced costs, and decreased court involvement in discovery disputes.

The *Primer* was a topic of dialogue at the WG1 meetings in 2019 and 2020, and an initial draft was distributed for member comment in 2021. The draft was revised based on member feedback and published for public comment in November 2021. Where appropriate, the comments received during the public comment period have been incorporated into this final version.

On behalf of The Sedona Conference, I thank drafting team leaders Rebekah Bailey and Don Myers for their leadership and commitment to the project. I also recognize and thank drafting team members Scott Borrowman, Kelly Cullen, MaryBeth Gibson, Jill Griset, Kristen Orr, and Michael Showalter for their dedication and contributions, and Steering Committee liaisons Lea Malani Bays, Jennifer Coleman, Greg Kohn, and Lauren Schwartzreich for their guidance and input. I also wish to recognize the Hon. Kristen L. Mix for serving as Judicial Observer to the drafting team.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; patent remedies and damages; patent litigation best practices; trade secrets; data security and privacy liability; and other "tipping point" issues in the law. 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. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
January 2022

TABLE OF CONTENTS

I. INTRODUCTION

The December 2015 amendments to the Federal Rules of Civil Procedure ("Rules") were crafted with the goal of reducing costs and delay by promoting cooperation among the parties, encouraging proportionality in the use of discovery tools, and supporting early and active judicial case management.[1] Judicial commentary and litigation experience demonstrate that the promised "just, speedy, and inexpensive determination of every action and proceeding" remains unachieved in many matters.[2] Change, however, was never going to happen overnight. Indeed, Chief Justice Roberts warned "[t]he practical implementation of the rules may require some adaptation and innovation."[3] Practitioners should proactively transform their discovery practices, starting with a heightened focus on discovery requests.

The 2015 amendments to Rule 34 were driven, in part, by concerns that objections to Rule 34 requests were not sufficiently specific, contributing to unreasonable discovery burdens.[4] In support of Chief Justice Roberts' call for adaptation

1. Memorandum from Hon. David G. Campbell, Advisory Committee on Civil Rules, to Hon. Jeffrey S. Sutton, Chair of Committee on Rules of Practice & Procedure, regarding Proposed Amendments to the Federal Rules of Civil Procedure (May 2, 2014).

2. *See* FED. R. CIV. P. 1.

3. U.S. Sup. Ct., 2015 Year-End Report on the Federal Judiciary 9 (Dec. 31, 2015).

4. FED. R. CIV. P. 34 advisory committee's note to 2015 amendment (stating "Rule 34(b)(2)(B) is amended to require that objections to Rule 34 requests be stated with specificity," and were intended to reflect amendments to Rule 34(b)(2)(C) that objections must specify the extent of objections and the nature of productions); *see also* The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 69 (2018) (comment 2e) [hereinafter *The Sedona Principles, Third Edition*].

and innovation, in March 2018, The Sedona Conference Working Group 1 published the *Federal Rule of Civil Procedure 34(b)(2) Primer*, which included practical pointers on responding to discovery requests, provided guidance on the revised Rules' push for early discovery conferences and increased court involvement, and provided a detailed framework for drafting responses to requests for production that comply with revised Rule 34(b)(2).[5]

The Rule amendments also provide an opportunity to explore one of the causes of poorly drafted Rule 34 responses—deficiencies with Rule 34 ***requests***. Indeed, vague and overbroad discovery requests have continued after the 2015 Amendments, clogging the courts and increasing litigation costs.[6] In response, The Sedona Conference Working Group 1 has prepared this *Primer on Crafting eDiscovery Requests with "Reasonable Particularity"* ("*Primer*") with the purpose of providing practical considerations for drafting requests for production in compliance with Rule 34(b)(1).

Rule 34(b)(1) has required parties to draft requests for production with "reasonable particularity" since 1970. Section II of this *Primer* explores the history of the phrase "reasonable particularity" as well as the case-specific circumstances that drive its definition. It then addresses the relationship between Rule 26 and Rule 34. A party's ability to obtain materials through Rule

5. *The Sedona Conference, The Sedona Conference Federal Rule of Civil Procedure 34(b)(2) Primer: Practice Pointers for Responding to Discovery Requests*, 19 SEDONA CONF. J. 447 (2018) [hereinafter *Federal Rule of Civil Procedure 34(b)(2) Primer*].

6. *See, e.g.*, Michael Kors, LLC v. Su Yan Ye, No. 2:18-cv-2684, 2019 WL 1517552, at *3 (S.D.N.Y. Apr. 8, 2019) ("The 2015 amendments to the Rules were designed to stop counsel from relying on standard, overbroad requests and to also require tailoring on the particular issues and circumstances in the case. Defendant clearly did not comply with its discovery obligations under Rules 1, 26, and 34 when propounding the requests.").

34 is constrained by the discoverability standard in Rule 26(b), which limits the scope of discovery to: "any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case."[7] Indeed, Rule 34 incorporates Rule 26(b)'s scope requirement by reference, stating: "A party may serve on any other party a request within the scope of Rule 26(b) . . . ." Moreover, drafting reasonably particular requests requires thoughtfulness and due diligence because Rule 26(g) treats an attorney's signature as a certification that the requests were formed "after a reasonable inquiry," and that the requests comply with the Rules.

Section II also explores how courts have addressed "reasonable particularity" at a time when the volume of discovery is increasing significantly. While a request for "all documents" may be convenient and may have been appropriate in the past, it may not be proportional to the needs of a case or set forth the information sought with "reasonable particularity" given the exponential growth of electronically stored information ("ESI").

Section III explains how to draft requests that satisfy the "reasonable particularity" standard. For example, counsel should consider focusing on the end result—i.e., on the information necessary to establish or defeat a claim or defense. Further, if the requesting party cannot articulate how the information sought relates to an allegation in the complaint or an affirmative defense, it should reconsider the request. Moreover, counsel should conference with opposing counsel to facilitate discussion about relevant topics for discovery, the sequence of discovery, proportionality considerations, likely sources of ESI, as well as sources of potential conflict and motion practice. The parties may also conference to discuss staging discovery,

7. FED. R. CIV. P. 26(b)(1).

focusing first on areas where there is little or no objection to the information sought and then expanding the requests as necessary.

Section IV provides a practical, example-based framework for how to draft requests for production in light of the renewed focus on "reasonable particularity." Suggestions include avoiding "form" requests as well as overbroad "boilerplate" definitions and instructions. Instead, requests should identify specific, identifiable, or discrete documents. This could include limiting requests to certain custodians or locations or requesting information using phrases such as "sufficient to show" rather than "any and all," where appropriate.

As explained throughout this *Primer*, drafting requests with "reasonable particularity" requires a heightened focus on requests that are specific to the needs of the case. A request cannot be particular if it is comprised of confusing or unnecessary instructions, boilerplate definitions, and template requests. In short, in preparing Rule 34 requests, a requesting party must understand its goals. The suggestions provided in this *Primer*, along with the *Federal Rule of Civil Procedure 34(b)(2) Primer*, are designed to promote efficient discovery, reduce costs, limit delays, and decrease court involvement in discovery disputes.

II. HISTORICAL AND LEGAL BACKGROUND

A. The Standard's Origin

Since 1970, Rule 34 has required parties requesting the production or inspection of documents to "describe with *reasonable particularity* each item or category of items" they seek to discover.[8] The concept of "reasonable particularity," however, was first introduced several decades earlier, in the 1946 Advisory Committee Notes' citation to two U.S. Supreme Court cases, *Consolidated Rendering Co. v. Vermont*,[9] and *Brown v. United States*.[10] These cases are helpful for understanding just how "particular" requests were originally required to be.[11]

In *Consolidated Rendering*, the requesting party served a notice, akin to a subpoena *duces tecum*, for documents concerning "business dealings" between the two identified parties during a specified time period.[12] On appeal, the U.S. Supreme Court heard arguments that "the documents [sought] were not described with the particularity required in the description of documents."[13] In the 1908 opinion, the U.S. Supreme Court acknowledged that the requests appeared "quite broad" as written, but the Court pointed out that they were limited to relevant

8. FED. R. CIV. P. 34(b)(1)(A) (as amended 2015) (emphasis added).

9. 207 U.S. 541 (1908).

10. 276 U.S. 134 (1928).

11. FED. R. CIV. P. 34, advisory committee notes to the 1946 amendment.

12. *Consolidated Rendering*, 207 U.S. at 554 (paraphrasing request as seeking "such books or papers as related to, or concerned, any dealings or business between January 1, 1904, and the date of the notice, October, 1906, with the parties named therein, who were cattle commissioners of the state of Vermont, and which papers were to be used relative to the matter of complaint pending").

13. *Id.* at 553–54.

documents during a specified period of time.[14] The Court saw "no reason why all such books, papers and correspondence which related to the subject of the inquiry, and were described with reasonable detail" were not discoverable.[15]

Similarly, in its 1928 decision in *Brown v. United States*, the U.S. Supreme Court addressed the reasonableness of a request seeking "all letters or copies of letters, telegrams, or copies of telegrams, incoming and outgoing" passed between one identified party and another during a specified time period relating to any of a list of eighteen broadly described topics.[16] The Supreme Court overruled the objections, reasoning "[t]he subpoena . . . specifies . . . with *reasonable particularity* the subjects to which the documents called for relate" and the time period at issue.[17]

---

14. *Id.* at 554 (analyzing a request for "books or papers as related to, or concerned any dealings or business between January 1, 1904, and the date of the [subpoena], with the parties named therein" and holding that these requests "related to the subject of inquiry, and were described with reasonable detail" and that responsive documents should be produced).

15. *Id.* Of course, this opinion was delivered almost a century before the explosion of ESI.

16. Brown v. United States, 276 U.S. 134, 138–39 (1928) (citing a long list of topics for the subject matter of the documents sought as exchanged between specified parties during particular time frames, including documents referencing general meetings, zone meetings, "costs of manufacture," "issuing new price lists," "exchanging price lists," "maintaining prices," "reducing prices," "curtailment of production," cost bulletins, and the intention of specific parties to attend a particular exposition).

17. *Id.* at 143 (emphasis added). The Court further contrasted the subpoena in question with that at issue in *Hale v. Henkel*, 201 U.S. 43 (1906). In contrast with *Brown*, the requesting party in *Hale* did not identify a date range or the subject matter of documents sought. The Court in *Hale* therefore ruled the requests to be "to [sic] sweeping to be regarded as [r]easonable [sic]," and that production of all such documents could "completely put a stop to the business of the company." *Id.* at 142–43 (citing *Hale*, 201 U.S. 43).

When the "reasonable particularity" concept moved from the Advisory Committee Notes to the text of the Rule in 1970, "leading commentators view[ed] the designation requirement as concerning identification" of documents, not as addressing the requests' scope or breadth.[18] In other words, a request that is not reasonably particular may be more appropriately objected to as vague or ambiguous.[19]

---

18. Mallinckrodt Chem. Works v. Goldman, Sachs & Co., 58 F.R.D. 348, 349, 354 (S.D.N.Y. 1973) (ordering production of "all documents submitted to the [SEC] in connection with the SEC's investigation of the financial collapse of the Penn Central Company" because "it is clear that defendant can identify the documents demanded by plaintiffs"); *see, e.g.*, Parsons v. Jefferson-Pilot Corp., 141 F.R.D. 408, 412 (M.D.N.C. 1992) (analyzing "reasonable particularity" by asking whether the "requests place the respondents on reasonable notice of what is called for and what is not"); *In re* Folding Carton Antitrust Liti*g.*, 76 F.R.D. 420, 424 (N.D. Ill. 1977) ("In our opinion, Request Nos. 49-51 comport with the reasonable particularity requirement of Rule 34 and defendants can identify the documents demanded by plaintiffs. The requests designate by well described categories and specific time periods the documents to be produced. This is all that is required under Rule 34."); United States v. Int'l Bus. Machs. Corp., 72 F.R.D. 78, 82 (S.D.N.Y. 1976) ("[T]he Request embraces a demand to government agencies for all documents relating to the 'employment' by the agencies, regardless of when that employment occurred, of any of the witnesses. Since all documents relating to an employee are theoretically concerned with his employment, on its face paragraph one demands every document[] in the 'employing' agency's possession which in any way mentions one of the witnesses. Since this construction would make much of if not all of the balance of the Request superfluous, the court must conclude that IBM in fact desires by this part of its demand less than every such document. What is desired is not reasonably particularized.").

19. *See, e.g.*, Lykins v. CertainTeed Corp., No. CIV.A. 11-2133, 2012 WL 3578911, at *9 (D. Kan. Aug. 17, 2012) (characterizing responding party's vague and ambiguous objections to document requests as taking issue with the request's lack of particularity). Note, however, that other courts have stressed the close connection between burden and "reasonable particularity." *See infra* discussion of *Regan-Touhy v. Walgreen Co.*, Section II.C.

Whether a request is "reasonably particular" under the Rules depends on the circumstances of the case, including the degree of knowledge that the requesting party may reasonably have about the documents sought when the request is made.[20] For example, a plaintiff-employee requesting documents from their defendant-employer is generally equipped with a greater understanding of the types of documents the employer may possess and how to most appropriately describe them to ensure that the employee obtains what it seeks. Conversely, a plaintiff-consumer or plaintiff-competitor, who only interacts with a defendant-corporation in rare, arm's lengths transactions, may have a much more difficult time describing which documents exist, how they are referenced, how they are stored, etc. Thus, whether a document request is properly drafted to meet the "reasonable particularity" requirement must be analyzed in the

---

20. *Mallinckrodt*, 58 F.R.D. at 353 ("The 'reasonable particularity' requirement is not susceptible to exact definition. What is reasonably particular is dependent upon the facts and circumstances in each case."). The Federal Practice & Procedure Manual concurs that the analysis of the "reasonable particularity" of a request:

> [n]ecessarily . . . must be a relative one, turning on the degree of knowledge that a movant in a particular case has about the documents it requests. . . . [T]he ideal is not always attainable and Rule 34 does not require the impossible. Even a generalized designation should be sufficient when the party seeking discovery cannot give a more particular description and the party from whom discovery is sought will have no difficulty in understanding what is wanted. . . . There have been a great many cases in which courts have relied on the requirement of designation as a ground for refusing to require a general search or inspection of voluminous records. . . . Such concerns are addressed more directly under the proportionality provisions added in 1993 and now found in Rule 26(a)(2)(C).

CHARLES ALAN WRIGHT, ET AL., 8A FEDERAL PRACTICE & PROCEDURE § 2211 at 415 (3d ed. Apr. 2020 update) [hereinafter WRIGHT].

context of the information available to the requesting party when making the request.

Of course, a poorly drafted request may also cause problems with overbreadth and burden. For example, a request seeking documents without specifying a time frame may lack particularity, and as a result, may ultimately seek voluminous, irrelevant documents outside the scope of the case—the production of which could be unduly burdensome. However, the concepts of particularity and breadth/burden are not directly synonymous and should be considered separately.[21]

As discussed in the Introduction, in 2015 Rule 34 was amended once again to require increased specificity when drafting *responses* to document requests, but the amendment did not provide any additional guidance regarding the "reasonable particularity" requirement for propounding requests.

B. Relationship Between Rule 26(g) and Rule 34

Counsel has an ethical obligation to serve Rule-compliant discovery requests.[22] As discussed in more detail in *The Sedona Principles, Third Edition*, three themes dominated the 2015 amendments: cooperation, proportionality, and increased judicial involvement.[23] Among other things, Rule 26(b) was amended to allow parties to obtain discovery "relevant to any party's claim or defense and proportional to the needs of the case" and delete the broad former language permitting "discovery of any matter relevant to the subject matter involved in the action" or that is "reasonably calculated to lead to the discovery

21. *Id.*; *see also* FED. R. CIV. P. 34, advisory committee notes to the 1970 amendment (stating the question of undue burden is best addressed by Rule 26 in "consideration of the needs of the party seeking discovery").

22. *See* Model Rules of Prof'l Conduct r. 3.4 (Am. Bar Ass'n 2020).

23. *The Sedona Principles, Third Edition*, *supra* note 4, at 30.

of admissible evidence."[24] Rule 34(a) permits a "request within the scope of Rule 26(b)," and therefore necessarily incorporates the relevance and proportionality elements of amended Rule 26(b)(1).[25]

One of the important reasons to keep the scope of discovery, including relevance and proportionality, in mind when drafting Rule 34 requests is that Rule 26(g) treats service of a discovery request as a certification. The requesting party and its counsel certify that each request is consistent with the Rules, not interposed for any improper purpose, and "neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action."[26] Courts have also held that the requesting party "bears the burden of fashioning the requests appropriately."[27] Sedona Principle 4 similarly provides that "Discovery requests for electronically stored information should be as specific as possible . . . ."[28]

The court in *Effyis, Inc. v. Kelly* ordered sanctions against the defendant for issuing overbroad requests, holding that the requests violated Rule 26(g) and that in such a case, the court *must* impose sanctions.[29] The court noted that the defendant issued

---

24. FED. R. CIV. P. 26(b)(1).

25. FED. R. CIV. P. 26, 34.

26. Mancia v. Mayflower Textile Servs. Co., 253 F.R.D. 354, 356 (D. Md. 2008) (quoting FED. R. CIV. P. 26(g)(1)(B)(iii)); *see also* Effyis, Inc. v. Kelly, No. 18-13391, 2020 WL 4915559 (E.D. Mich. Aug. 21, 2020) (imposing sanctions on defendant's counsel under Rule 26(g)(3) for serving discovery requests "unbounded by time, relevance, or reason").

27. *See, e.g.*, Peterson v. Hantman, 227 F.R.D. 13, 17 (D.D.C. 2005) (finding no error when responding party responded to the "letter" of requests that were originally "misworded").

28. *The Sedona Principles*, *Third Edition*, *supra* note 4, at 51.

29. *Effyis*, 2020 WL 4915559, at *1–2.

98 separate requests, and they all began with "any and all" and were not limited by time or scope.[30] The court also noted that the definition of "document" in the requests stretched over a page in length.[31] One document request that the court found especially egregious sought "[a]ny and all DOCUMENTS in Plaintiff's possession, custody, or control which reflect or relate to any meetings Plaintiffs, Plaintiff's employees, or Plaintiff's agents had with Darren Kelly including any handwritten or typed notes."[32] The court said that the request was so broad, it would take an "extreme 'subjective guessing game' to understand whether a document—as broadly defined in the request—relates to 'any' meetings that anyone involved with Plaintiffs had with Defendant."[33] The magistrate judge's report and recommendations proposed a finding of a violation of Rule 26(g), but the district court went further, sanctioning the defendant by requiring the defendant to pay the plaintiff's attorneys' fees.[34]

As the court said in *Bottoms v. Liberty Life Assurance Co. of Boston*, Rule 26(g) "obligates each attorney to stop and think about the legitimacy of a discovery request, a response thereto, or an objection."[35] Counsel does not satisfy Rule 26(g) by "robotically recycling discovery requests" used in other cases.[36] In *Bottoms*, which involved claims brought under the Employment Retirement Income Security Act, the court cited numerous examples of the plaintiff's failure to comply with Rule 26(g). For

30. *Id.* at *2.

31. *Id*.

32. *Id*.

33. *Id*.

34. *Id.* at *1.

35. Bottoms v. Liberty Life Assurance Co. of Boston, No. 11-cv-01606, 2011 WL 6181423, at *4 (D. Colo. Dec. 13, 2011) (quoting High Point Sarl v. Sprint Nextel Corp., No. 09-2269, 2011 WL 4036424, at *11 (D. Kan. Sept. 12, 2011)).

36. *Bottoms*, 2011 WL 6181423, at *5.

example, in one request, the plaintiff asked the defendant to produce complete personnel files for every person "who was in any way involved in the handling, processing or denial of Plaintiff's claim for benefits."[37] The court said that such a request swept too broadly, as it failed to distinguish between the defendant's employees involved in clerical activities (e.g., the handling of the plaintiff's claim), and the decision-makers responsible for denying plaintiff's claim.[38]

Despite these ethical obligations and requirements in the Rules and case law, counsel routinely issue overbroad, noncompliant discovery requests, and cases often get bogged down in costly discovery disputes, leading to protracted, expensive litigation.[39] The 2015 amendments were an attempt to curb these abuses.[40] Crafting document requests that specify the items

37. *Id.* at *6.

38. *Id*.

39. *Id*. at *4 ("Despite the requirements of [Rule 26(g)], however, the reality appears to be that with respect to certain discovery, principally interrogatories and document production requests, lawyers customarily serve requests that are far broader, more redundant and burdensome than necessary to obtain sufficient facts to enable them to resolve the case through motion, settlement or trial."); *see also* Legends Mgmt. Co. v. Affiliated Ins. Co., 2:16c-v-01608-SDW-SCM, 2017 WL 4618817, at *2 (D.N.J. Oct. 13, 2017) ("[T]he sole purpose of discovery is to add flesh for trial on the parties' respective claims and defenses in the given action"); Adams v. City of Chicago, No. 06 C 4856, 2011 WL 856589, at *3 (N.D. Ill. Mar. 9, 2011) ("[A] lawsuit is about deciding the particular rights and liabilities of these parties arising out of these events, not about discovery for its own sake.").

40. *Federal Rule of Civil Procedure 34(b)(2) Primer*, *supra* note 5, at 452; *see also* Michael Kors, LLC v. Su Yan Ye, No. 2:18-cv-2684, 2019 WL 1517552, at *3 (S.D.N.Y. Apr. 8, 2019) ("The 2015 amendments to the Rules were designed to stop counsel from relying on standard, overbroad requests and to also require tailoring on the particular issues and circumstances in the case.").

sought with "reasonable particularity" provides an additional opportunity to achieve this goal.

C. "Reasonable Particularity" in the Age of Electronic Discovery

As discussed in the preface to *The Sedona Principles, Third Edition*, there has been an "explosion in the volume and diversity of forms of electronically stored information," a "constant evolution of technology applied to eDiscovery," and litigation experience dealing with eDiscovery that have demonstrated both the complications and benefits of electronic discovery.[41] Because most discovery of ESI is conducted under Rule 34, it is appropriate to consider specifically how "reasonable particularity" applies to electronic discovery.[42]

As electronic discovery emerged in the 21st century and the volume of ESI exploded, the need for compliance with the "reasonable particularity" requirement became more pronounced. The Tenth Circuit recognized in *Regan-Touhy v. Walgreen Co.* that "the burdens and costs associated with electronic discovery, such as those seeking 'all email,' are by now well known . . . ."[43] *Regan-Touhy* cautioned courts to prevent collateral discovery disputes from shifting focus away from the merits of the case.[44] *Reagan-Touhy* and the additional cases discussed below illustrate courts' application of Rule 34's "reasonable particularity" requirement in the age of electronic discovery.

---

41. *The Sedona Principles, Third Edition*, *supra* note 4, at 8.

42. Non-party electronic discovery is conducted under Rule 45, which is subject to the same limitations as those imposed by Rule 34. FED. R. CIV. P. 45, advisory committee notes to the 1991 amendment; *see also* Gutierrez v. Mora, No. CV 18-781-KS, 2019 WL 8953125, at *5 (C.D. Cal. Dec. 18, 2019) ("the scope of document production under Rule 45 is governed by the same standards as production under Rule 34").

43. Regan-Touhy v. Walgreen Co., 526 F.3d 641, 649 (10th Cir. 2008).

44. *Id*.

1. Requests for "All Communications" and "All Documents"

The proliferation of electronic communications and the large volumes of electronic documents maintained by organizations have led courts in some cases to reject requests that seek "all communications," or "all documents" on the grounds that they fail Rule 34's "reasonable particularity" requirement. In *Regan-Touhy*, for example, the plaintiff claimed that an employee at Walgreen's used her position to access the plaintiff's pharmacy records and then disclosed the records to her ex-husband and others.[45] The plaintiff's document requests sought a copy of the employee's entire personnel record, all communications between Walgreen's and the employee, and all documents that mentioned or related in any way to the employee.[46] The plaintiff filed a motion to compel Walgreen's to produce documents responsive to the request, which was denied by the trial court.[47] On appeal, the circuit court affirmed the lower court's ruling, holding that the request for "all communications" was not narrowly tailored and could have been more focused on whether Walgreen's disciplined its employee for disclosing the plaintiff's condition.[48] While some of the opinion focused on the overbreadth and burden of the requests, the court recognized that overbreadth and burden are closely tied to the "reasonable particularity" requirement. The court recognized that while litigants enjoy broad discovery privileges, "with those privileges come certain modest obligations, one of which is the duty to state discovery requests with 'reasonable particularity.' All-encompassing demands of this kind take little account of that

45. *Id.* at 644.

46. *Id.* at 648–49.

47. *Id.* at 646.

48. *Id.* at 649, 653.

responsibility."[49] The court explained that what qualifies as "reasonably particular" depends on the circumstances of each case, but at a minimum, the request must "apprise a person of ordinary intelligence what documents are required and [enable] the court . . . to ascertain whether the requested documents have been produced."[50]

Other courts have held that "[a]ll-encompassing demands that do not allow a reasonable person to ascertain which documents are required do not meet the particularity standard of Rule 34(b)(1)(A)."[51] Broad requests that seek all documents that "refer or relate" to the allegations in the complaint, particularly when the complaint asserts broad allegations, may not satisfy the "reasonable particularity" requirement.[52] Conversely, a request that sought documents that "refer or relate to [the plaintiff's allegedly involuntary] retirement," was valid, as "there was no mystery" to what documents plaintiff requested, and the request identified a narrow category of documents related to the elimination of the plaintiff's position.[53] The court said that requests "should be reasonably specific, allowing the respondent

49. *Id.* at 649 (citation omitted) (addressing the request for "all documents . . . that refer to, mention or relate in any way to Plaintiff, Whitlock, or the litigation or the allegations, facts and circumstances concerning the litigation").

50. *Id.* at 649–50 (quoting WRIGHT, *supra* note 20, at 415); *see also* Lopez v. Don Herring Ltd., 327 F.R.D. 567, 575 (N.D. Tex. 2018) (noting that the "reasonable particularity" requirement in the Rule must describe the documents "sufficient to apprise a man of ordinary intelligence which documents are required." (citations omitted)).

51. *In re* Milo's Kitchen Dog Treats Consol. Cases, 307 F.R.D. 177, 179–80 (W.D. Pa. 2015) (quoting *In re* Asbestos Prods. Liab. Litig. (No. *180 VI), 256 F.R.D. 151, 157 (E.D. Pa. 2009)).

52. *See, e.g.*, Dauska v. Green Bay Packaging, Inc., 291 F.R.D. 251, 261–62 (E.D. Wis. 2013).

53. *Id.* at 262.

to readily identify what is wanted."[54] Requests that are "all inclusive of a general topic function like a giant broom, sweeping everything in their path, useful or not," are accordingly problematic.[55] They "require the respondent either to guess or move through mental gymnastics which are unreasonably time-consuming and burdensome to determine which of many pieces of paper may conceivably contain some detail, either obvious or hidden, within the scope of the requests."[56]

2. Setting a Time Period for the Requests

Requests that seek broad categories of documents concerning events that occurred over a very short time period may satisfy the "reasonable particularity" standard.[57] One court held that requests for production that sought "any and all" documents and communications regarding events described in the complaint, where the events took place over a couple of hours and involved the policies and practices of a single state agency, were "sufficiently particular."[58] Where communications related to a lawsuit are relevant, a request seeking production of communications with third parties related to the lawsuit may be sufficiently restricted in time (i.e., the duration of the lawsuit) that the time frame is reasonably particular.[59] Another court

54. *Id.* at 261.

55. *Id*. (quoting Audiotext Commc'ns v. U.S. Telecom, Inc., No. CIV A. 94–2395–GTV, 1995 WL 18759, *1 (D. Kan. Jan. 17, 1995)).

56. *Id*.

57. Freedom Found. v. Sacks, No. 3:19-CV-05937-RBL, 2020 WL 2219247, *2 (W.D. Wash. May 7, 2020).

58. *Id*.

59. *See, e.g.*, Boehm v. Scheels All Sports, Inc., No. 15-cv-379-jdp, 2016 WL 6811559, *2 (W.D. Wis. Nov. 17, 2016) (holding that informal discovery requests, which the court evaluated under Rule 34, seeking "your client's or your firm's communications with [certain third parties] related to this

similarly held that a request that was limited to a discrete time period—two years—was "reasonably particular."[60]

Yet, even shorter time periods may be viewed as not reasonably particular in certain contexts. For example, a six-month period may be too long if the requesting party seeks broad categories of sensitive information. One court considered a request for all Facebook posts for a six-month period relating to "Plaintiff's activities or mental status."[61] In evaluating the request, the court held that the information requested must be described with "reasonable particularity," and that "[t]he test for reasonable particularity is whether the request places a party upon 'reasonable notice of what is called [f]or and what is not.'"[62] The court ordered the defendant to request specific items from the plaintiff's Facebook or other social media accounts relating to physical activities or mental status in a six-month period.[63]

In sum, the requirement to identify documents with "reasonable particularity" should not require the producing party "to ponder and to speculate in order to decide what is and what

lawsuit" provided sufficient information to allow the defendant to identify responsive documents and therefore satisfied the "reasonable particularity" requirement.) However, the duration of the lawsuit may impact whether the time period is sufficiently particular.

60. Guerra v. Balfour Beatty Communities, LLC, No. EP-14-CV-268-DB, 2015 WL 13794439, at *6-7 (W.D. Tex. Nov. 19, 2015) (holding that because Plaintiff limited request 31, which sought "all agreements between the United States government, or any of its agencies, and Defendant in regards to Defendant's operations at its Fort Bliss and White Sands Missile Range locations" for a period of 2 years, and because it related to a subject integral to her claim, it was reasonably particular and not overbroad).

61. Locke v. Swift Transp. Co. of Ariz. LLC , No. 5:18-CV-00119, 2019 WL 430930, at *1 (W.D. Ky. Feb. 4, 2019).

62. *Id.* at *2 (citations omitted).

63. *Id.* at *5.

is not responsive."[64] "Broad and undirected" requests for all documents that in any way relate to the complaint are generally inappropriate.[65] "A request for 'all documents and records' that relate to 'any of the issues [in the lawsuit],' while convenient, fails to set forth with reasonable particularity the items or category of items sought for [the responding party's] identification and production of responsive documents."[66] One court described an adequate request as one that "describes items with 'reasonable particularity'; specifies a reasonable time, place, and manner for the inspection; and specifies the form or forms in which electronic information can be produced."[67] A properly drafted request will describe the items or category of items sought with a level of detail that the requesting party should be reasonably expected to know. Thus, a request is sufficiently clear if it "places the [responding] party upon reasonable notice of what is called for and what is not."[68]

---

64. Bruggeman v. Blagojevich, 219 F.R.D. 430, 436 (N.D. Ill. 2004); *see also* Judge Virginia A. Phillips & Judge Karen L. Stevenson, Rutter Group Practice Guide: Federal Civil Procedure Before Trial, California & Ninth Circuit Edition § 11:1886 (2020 ed.) ("[T]he apparent test is whether a respondent of average intelligence would know what items to produce.").

65. Lopez v. Don Herring Ltd., 327 F.R.D. 567, 575 (N.D. Tex. 2018) ("'[B]road and undirected requests for all documents which relate in any way to the complaint' do not meet Rule 34(b)(1)(A)'s standard." (quoting Parsons v. Jefferson-Pilot Corp., 141 F.R.D. 408, 412 (M.D.N.C. 1992))).

66. *Id*. (quoting Sewell v. D'Alessandro & Woodyard, Inc., No. 2:07-CV-343-FTM-29, 2011 WL 843962, at *2 (M.D. Fla. Mar. 8, 2011)).

67. Pearson v. Bakersfield Police Dep't, No.: 1:18-cv-00372 - JLT, 2019 WL 1765279, at *2 (E.D. Cal. Apr. 22, 2019) (citation omitted) (quoting Kidwiler v. Progressive Paloverde Ins. Co., 192 F.R.D. 193, 202 (N.D. W. Va. 2000)).

68. *Id.* Note too that some courts have local rules that require specificity in the requests. *See, e.g.*, Glass Egg Digital Media v. Gameloft, Inc., No. 17-cv-04165-MMC(RMI), 2019 WL 5720731, at *2 (N.D. Cal. Nov. 5, 2019) ("Regarding discovery in general, and motions to compel in particular, Northern District Local Civil Rule 37-2 makes it incumbent on a party moving to compel

discovery to 'detail the basis for the party's contention that it is entitled to the requested discovery and show how the proportionality and other requirements of Fed. R. Civ. P. 26(b)(2) are satisfied.'").

III. DRAFTING REQUESTS THAT SATISFY THE REQUIREMENT

Given the increased complexity of modern discovery and the evolving case law, how should practitioners draft requests to comply with the Rules? The following are practice considerations to help attorneys balance these concerns.

A. Start at the End: Focus on Information Needed for Claims and Defenses

It may be useful to start at the end: focus on information necessary to establish or defeat a claim or defense, deal with pertinent collateral issues (e.g., standing, jurisdiction, or class certification), win summary judgment, or succeed at trial. Jury instructions often are a good starting place to evaluate the required elements of each claim and defense. Other documents to review include the complaint, Rule 12 motions, the answer, and initial disclosures. Consider compiling a list of document categories and asking: How are the documents sought helpful? If an answer or initial disclosure does not contest a factual assertion in the complaint, there may be no need to request information relevant to that factual assertion. Or, if an answer or initial disclosure identifies the nature of a dispute, the requesting party can focus on that dispute.

Clients will benefit from this early time investment that will yield "just, speedy, and inexpensive" results through reasonably particular requests. As counsel drafts each request, it should consider how the information sought relates to a claim or defense. If counsel cannot articulate such a relationship, it should reconsider the request. Counsel might also consider having a colleague review the requests and point out likely objections so that those might be proactively addressed in the drafting of the request. By articulating the reason for each request and how it ties to a claim or defense, counsel will be well prepared to confer with opposing counsel and for any hearings on a motion for

protective order or motion to compel. Counsel will strengthen professional relationships with judges and opposing counsel by propounding thoughtful requests.

B. Resources to Consider that Do Not Require Discussions with Opposing Counsel

Counsel should talk with its client about drafting requests. For example, in an employment wage-and-hour case, the plaintiff may know what systems were used for timekeeping records and the type of detailed information those systems contain. In a dispute between two companies that have had a business relationship, one company may similarly have information about the other company's relevant systems based on that relationship. If a client has information about relevant sources of information that an opposing party is likely to have, counsel can serve targeted requests for that information. The client may also have information about specific people involved in the matter that may guide requests for production of communications and can inform the relevant time period for different requests.

Counsel should also consider using publicly available resources to find out as much about the responding party as possible to aid in the drafting of reasonably particular requests. Potential sources to consider include the responding party's website or online sources of information, marketing materials distributed by the responding party, or publicly available filings with government agencies.

C. Meet and Confer with Opposing Counsel

Conferences between the parties can also help counsel craft or refine requests that do not impose unreasonable discovery burdens. As discussed in the *Federal Rule of Civil Procedure 34(b)(2) Primer*, a "substantive conference between the parties early in the case provides an opportunity to comply with the

Rules amendments and avoid disputes about requests for production or responses to those requests."[69] Several courts provide guidelines for conducting discovery conferences.[70]

Early conferences among the parties can help facilitate discussion about the scope of discovery, including relevance and proportionality, sequence of discovery, areas of inquiry that are least likely to draw objection, and those where motion practice is likely. For example, in a putative consumer products liability class action, the plaintiff may seek to represent consumers nationwide. However, the manufacturer may believe discovery should be limited to a particular state because of different marketing or distribution arrangements that are relevant to the claims or defenses. Even if the parties are unable to agree on the scope of discovery without some initial discovery, these conversations can facilitate staging discovery to focus first on locations to which there is no objection and then expanding, as necessary, as additional facts are learned.

Early conferences can also assist where requesting counsel may have limited information about the responding party's systems or may misunderstand the responding party's ability to easily produce requested documents. Where this is the case, the parties may find it helpful to conference early to better understand how requests should be tailored. While some "any and

69. *Federal Rule of Civil Procedure 34(b)(2) Primer*, *supra* note 5.

70. For example, the Northern District of California, the Northern District of Illinois, and the District of Colorado publish guidelines that include checklists for conversations about eDiscovery. *See* https://cand.uscourts.gov/forms/e-discovery-esi-guidelines/; https://www.ilnd.uscourts.gov/Pages.aspx?jYyawIFLXKMJrmXzxFk8lw==; http://www.cod.uscourts.gov/Portals/0/Documents/Forms/CivilForms/E-Discovery_Guidelines.pdf.

all" requests are objectionable, courts may approve of "all" language when limited to certain categories of information.[71]

D. Staging Requests

Sending a small number of targeted requests early in a case may quickly provide access to documents that may assist in crafting additional compliant requests. Consider, for example, a product liability suit alleging a design-related failure in a system component. Targeted requests for design drawings showing the component may result in quick access to core documents for consulting experts, who can then assist with crafting additional document requests. Moreover, opposing counsel may be less likely to ask for an extension of time in responding to a small number of targeted requests, allowing the parties to begin substantive discovery earlier. Such targeted requests may even lead to resolution of some claims or early settlement discussions.

When considering staging discovery requests, it is often useful to discuss the proposed process with opposing counsel. Doing so can help set expectations about the staging process and potential time frames. The parties may include information

71. *Compare* St. Paul Reins. Co. v. Com. Fin. Corp., 198 F.R.D. 508, 512–13 (N.D. Iowa 2000) (approving "all documents identified, or relied on" in a party's answers to a counterclaim plaintiff's first set of interrogatories directed to the counterclaim defendant), *and* Mallinckrodt Chem. Works v. Goldman Sachs & Co., 58 F.R.D. 348, 354–55 (S.D.N.Y.) (approving request for "all" documents submitted to the Securities and Exchange Commission in connection with a particular SEC investigation), *with* Frank v. Tinicum Metal Co., 11 F.R.D. 83, 85 (E.D. Pa. 1950) ("[A] blanket request . . . for the production of all books and records related to the subject matter is obviously too general and indefinite to be granted." (citation omitted)).

about proposed or agreed staged discovery in a Rule 26(f) case management statement or other filing with the court.[72]

E. Early Delivery of Rule 34 Requests

The 2015 amendments allow delivery (to be distinguished from "service") of Rule 34 requests 21 days after service of the complaint.[73] The Advisory Committee Notes acknowledge that this allows delivery of requests *before* an answer or Rule 12 motion is filed, but they explain that the revised timeline was "designed to facilitate focused discussion during the 26(f) conference" that "may produce changes in the requests."[74]

Early delivery of Rule 34 requests permits the parties to engage in specific discussions about potential objections to the requests, including relevance, scope, and proportionality, and strategies for resolving those objections as early as the Rule 26(f) discovery conference.[75] For example, after understanding what a requesting party is seeking, a responding party may disclose searches it would be willing to make to identify potentially responsive materials. Conferring about early Rule 34 requests provides the requesting party with an opportunity to further revise and refine its requests and reserve further requests for after consideration of the responding party's questions, concerns, and likely objections.

---

72. The discovery plan required by Rule 26(f)(3) requires, among other things, a discussion of "the subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused on particular issues." FED. R. CIV. P. 26(f)(3).

73. FED. R. CIV. P. 26(d)(2).

74. FED. R. CIV. P. 26, advisory committee's notes to the 2015 amendment.

75. *See* Philip Favro, *Navigating the Discovery Chess Match Through Effective Case Management*, 53 AKR. L. REV. 31, 45 (2019) (discussing the salutary effect of early Rule 34 requests on streamlining discovery).

F. Other Considerations

Counsel should consider whether there may be unintended consequences associated with the requests. For example, overly broad requests, especially those that use "any and all" or similar language, may prompt a producing party to produce documents in a "document dump," which can increase the requesting party's burden and cost associated with reviewing the documents. A requesting party's counsel should also consider whether its request calls for discoverable materials that may create unnecessarily higher discovery costs for both parties and even draw a cost-shifting request. Counsel also should consider how it would respond if the other party parroted back the structure or substance of the requests in requests to its own client. For example, in a lost-profits case, both parties are likely to request the other party's financial statements. If the requesting party is willing to produce the financial statements but objects to a request for "any and all documents related to" those financial statements, the requesting party should consider limiting its own request to just the financial statements.

Courts have mostly opted for practical solutions over sanctions when examining poorly drafted requests. For example, courts may order the parties to meet and confer over the scope of the request at issue. Courts may redraft a problematic request and compel production of a much narrower set of documents, which may or may not include pertinent documents the requesting party needs to prove its case.[76] Still other courts may refuse to compel production of documents responsive to a request lacking in particularity, partly in recognition that it is not the

76. *Cf.* William A. Gross Constr. Assocs., Inc. v. Am. Mfrs. Mut. Ins. Co., 256 F.R.D. 134, 135 (S.D.N.Y. 2009) (observing in a dispute over search terms that the court was placed "in the uncomfortable position of having to craft a keyword search methodology for the parties.").

court's job to revise requests for production.[77] Such a result could have dire consequences for a requesting party, especially when the documents sought are necessary to support claims or defenses.

Sanctions are nonetheless a real possibility for counsel drafting overbroad and voluminous requests, as the *Effyis* decision, discussed above, demonstrates.[78] However, in analyzing a request for production and in deciding an appropriate solution for an overbroad request, the parties and the court should take into consideration whether and how informational asymmetry constrained the requesting party's ability to more narrowly draft the request.[79]

77. *Cf.* McMaster v. Kohl's Dep't Stores, Inc., No. 18-13875, 2020 WL 4251342 at *3 (E.D. Mich. July 24, 2020) (rejecting the parties' request to select one of their competing lists of search terms and reasoning that the court had "no interest in going where angels fear to tread.").

78. Effyis, Inc. v. Kelly, No. 18-13391, 2020 WL 4915559, at *2 (E.D. Mich. Aug. 21, 2020).

79. Mallinckrodt Chem. Works v. Goldman, Sachs & Co., 58 F.R.D. 348, 353 (S.D.N.Y. 1973); WRIGHT, *supra* note 20, at 415.

IV. PRACTICE CONSIDERATIONS

Practice considerations for drafting requests that satisfy the "reasonable particularity" requirement are outlined below. In light of the focus in the Rules and this *Primer* on considering the needs of individual cases, these practice considerations should be evaluated with that aim in mind. Further, one size does not fit all—each case will be different and will be impacted by the nature of the parties in dispute (large organizations, individuals, government, etc.), the time frame for the facts (events that occurred over many years or a few days), the amount of ESI the parties retain, and myriad other factors. Nevertheless, by accounting for the topics listed below, counsel is more likely to satisfy the "reasonable particularity" requirement and ultimately obtain the right documents needed to prosecute or defend the case.

A. Avoid Reusing Form Requests

Requesting parties often duplicate their own template discovery requests, which cannot, by definition, be "particular." This practice may be motivated by concern that anything less than broad and voluminous requests will result in missing key information. Inexperienced attorneys may also rely on form discovery requests because they either do not know what they will need to prove or defend their case or they have not been properly trained by more seasoned counsel. Yet "[w]here the propounding counsel has made little effort to tailor the [requests] to the facts and circumstances" of the case, it should be no surprise that the other party responds with objections.[80]

80. Robbins v. Camden City Bd. of Educ., 105 F.R.D. 49, 56–57 (D.N.J. 1985) (criticizing the use of pattern interrogatories that are based on little more than "some word-processing machine's memory of prior litigation").

Referred to colloquially as "garbage in, garbage out,"[81] this practice of "robotically recycling discovery requests propounded in earlier actions" also violates Rule 26(g) obligations.[82]

The discovery process is designed to obtain the relevant facts essential to the case. Rote reliance on forms or templates fails to consider the factual nuances of each lawsuit. Vague and overbroad Rule 34 requests delay production and create disruptive disputes. Moreover, overbroad requests often lead to motion practice that derails discovery, clogs the courts, and increases litigation costs.[83] To promote the "just, speedy, and inexpensive" resolution of cases in accordance with Rule 1, counsel should take the time to think about how each discovery request advances the goal of obtaining evidence necessary to advance the matter.

---

81. *Cf.* United States v. Esquivel-Rios, 725 F.3d 1231, 1234 (10th Cir. 2013) ("Garbage in, garbage out. Everyone knows that much about computers: you give them bad data, they give you bad results."); Moyle v. Liberty Mut. Ret. Benefits Plan, No. 10-cv-2179, 2013 WL 100281 at *2 (S.D. Cal. Jan. 7, 2013) ("The Court has been asked to rule and it will do so. The result, considering the confusing, incomplete mishmash before the Court, may be a function of the old adage, 'garbage in, garbage out.'").

82. Bottoms v. Liberty Life Assurance Co., No. 11–cv–01606, 2011 WL 6181423 at *5 (D. Colo. Dec. 13, 2011) (observing that this "approach to discovery would be antithetical to the 'stop and think' mandate underlying Rule 26(g).").

83. *See* Caves v. Beechcraft Corp., No. 15-CV-125-CVE-PJC, 2016 WL 355491, at *2 (N.D. Okla. Jan. 29, 2016) (denying motion to compel and sustaining defendant's objections to document requests seeking "any and all" testimony concerning any "other litigation" as "clearly objectionable" because "[n]either Defendants nor the Court should have to guess what Plaintiff is really seeking. Nor is it the Court's job to redraft Plaintiff's discovery requests.").

B. Avoid Overbroad or Boilerplate Instructions and Definitions

An important part of drafting Rule-compliant requests is determining whether and/or how to include instructions and definitions. Instructions and definitions should be used sparingly and deliberately to clarify, reduce misinterpretation, or establish broad parameters for the corresponding requests. When used properly, instructions and definitions can be a useful tool for providing further particularity to requests. When used thoughtlessly, instructions and definitions can unnecessarily complicate discovery requests and draw objections.

Instructions should provide context to the requests collectively. To the extent an instruction obligates a responding party to do more than required under applicable Rules or accompanying Advisory Committee Notes, the instruction should include supporting legal authority. Additionally, consider including an instruction that the requests should not be construed to seek production of attorney-client privileged or work-product documents, but simply that such withheld documents should be reflected on a privilege log. This should obviate the need for the responding party to object to production of privileged documents. Instructions related to date ranges are also encouraged, making clear that all requests, unless specifically stated otherwise, should be interpreted to seek documents relevant to an identified date range.[84] Requests that specify no time frame are more likely to draw an objection. Lastly, instructions that specify the format of production pursuant to Rule 34(b)(1)(C) could be used if the parties have not previously agreed to a form of production. This is particularly true for productions of ESI that

84. *See* Wells Fargo Bank NA v. Wyo Tech Inv. Grp., LLC, No. CV-17-04140-PHX-DWL, 2019 WL 5653425, at *8 (D. Ariz. Oct. 31, 2019) (resolving dispute about time frame covered by discovery requests referencing instructions when relevant to deciding whether defunct organization had to produce historical financial records).

are difficult to extract in a user-friendly format or ESI produced from emerging technologies.

Unfortunately, instructions have been overused and abused in practice. Requesting parties commonly propound instructions that contain obligations greater than, or in conflict with, the requirements of Rule 34 or state rule equivalents.[85] Requesting parties should resist the urge to include these commonly used (but also commonly ignored) instructions, and instead turn them into interrogatories. An example of an instruction that would be a good candidate for an interrogatory would be one that asks the responding party to identify known responsive documents that are in the possession, custody, or control of a third party. Likewise, instructions that go beyond the requirements of Rule 26(b)(5)—for example, requiring the responding party to identify specific metadata or attributes of a document on a privilege log—would be better addressed through meeting and conferring in good faith.

Similarly, the definition section should provide further clarity by defining phrases and words that are truly open to disagreement or confusion. For example, the section may define case-specific words or phrases so that the parties all understand the scope of what is being sought. As with instructions, definition sections are commonly misused and abused.

Requests often include unnecessary definitions of common words or known terms of art. Consider instead a catch-all instruction that directs the responding party to attribute ordinary meaning to commonly used words or cite the regulations or case

85. *See* Calcor Space Facility, Inc. v. Super. Ct., 61 Cal. Rptr. 2d 567, 569 (Cal. Ct. App. 1997) (issuing a writ of mandate vacating trial court orders requiring a non-party's compliance with plaintiff's subpoena and finding that plaintiff's "six pages of 'definitions' and 'instructions' is particularly obnoxious . . . [and] in effect, turns each of the 32 requests into a complicated 'category' described in more than 6 pages.").

law that define applicable terms of art. Avoid defining words that already enjoy a standard definition. For example, requests often define "Document" by listing every conceivable type of physical evidence and ESI,[86] but Rule 34(a)(1)(A) already includes a definition for "documents or electronically stored information." Of course, a more specific definition of "document" may be appropriate where the requesting party can tailor its request to the specific types of relevant documents or ESI. Also, if the matter is in a state court where there is no equivalent state-law definition for "document," a requesting party may consider simply defining "document" by citing Rule 34(a)(1)(A) in the Federal Rules.

Poorly drafted definitions may render a request nonspecific and objectionable because the definition of a term used by the request is so overbroad. For example, a definition of "You" that includes third parties may exceed the proper scope of Rule 34's possession, custody, or control standard, rendering every request using that term improper by seeking information that can only be obtained via Rule 45 subpoena. Defining terms that do not appear in the requests themselves is not reasonably particular—unless of course, the term relates to a statutory claim in litigation, and the definition could be helpful.

When improperly drafted, definitions and instructions can make an otherwise appropriate request unreasonable, unduly burdensome, or otherwise improper under Rule 26(g). Well-crafted definitions and instructions can make requests clearer by, for example, defining the relevant time period for the requests or a term based on a statutory definition. A requesting

86. *See* Effyis, Inc. v. Kelly, No. 18-13391, 2020 WL 4915559 at *2 (E.D. Mich. Aug. 21, 2020) (imposing sanctions on counsel for propounding unreasonable document requests and spotlighting as particularly problematic the more than one-page definition for the word "document").

party should consider several questions before drafting an instruction or definition:

- Are the definitions and instructions merely copied from a prior request? If so, pursuant to the discussion above, the request may not be reasonably particular.
- Does the instruction request ESI that is proportional to the needs of the case? Particularly egregious instructions such as requiring a responding party to search for documents not in its possession, custody, or control "exceed or contradict the requirements of the Rules, [and use] definitions that are not actually used in the requests . . . ."[87]
- Is the source of ESI sought reasonably accessible, or will it create undue burden or cost?[88] For example, avoid (unless necessary) an instruction that the responding party must search deleted data, slack space, random access memory ("RAM"), disaster recovery tapes, and other nonprimary sources of ESI that may not be readily or reasonably accessible in the normal course.[89] Similarly, instructions asking a party to itemize each document responsive to the discovery requests that may have existed at a point in time and now no longer exists may be unduly burdensome or seek information that is impossible to provide.

87. *Federal Rule of Civil Procedure 34(b)(2) Primer*, *supra* note 5, at 464.

88. *The Sedona Principles, Third Edition*, *supra* note 4, at 138–40.

89. FED. R. CIV. P. 26(b)(2)(B)*; see The Sedona Principles, Third Edition*, *supra* note 4, at 134–43.

- Does the instruction contemplate production of documents that "can be obtained from some other source that is more convenient, less burdensome, or less expensive?"[90] If a requesting party believes that there is a basis for demanding that the responding party engage in such a search, it may be useful to meet and confer about such an instruction before issuing the discovery requests.
- Do the definitions include words that have commonly understood but unnecessary definitions, such as "and," "concerning," or "refer," especially where the special definition varies from the commonly understood definition?[91]
- Have the definitions and instructions complicated the request to such an extent that the request is akin to an interrogatory?[92]

---

90. FED. R. CIV. P. 26(b)(2)(C)(i).

91. For example, definitions of "concerning" sometimes purport to seek documents that "explicitly or implicitly, in whole or in part, reflect, refer to, record, regarding, are connected with, relate, describe, discuss, mention" and other verbs topics covered by the request. *See, e.g.*, CS Bus. Sys., Inc. v. Schar, No. 5:17-cv-86-Oc-PGBPRL, 2017 WL 8948376, at *3 (June 15, 2017) (describing a definition of "concerning" as "expansive" where it included "in addition to its commonly understood meanings, analyzing, comprising, concerning, constituting, dealing with, demonstrating, discussing, evidencing, explaining, Concerning [sic], pertaining to, providing, referencing, reflecting, regarding, relating to, revealing, supporting, showing, providing, and/or disproving"). Requests for materials that implicitly relate to a topic may add unnecessary subjective considerations into the request.

92. *See* Facedouble, Inc. v. Face.com, Inc., No. 12CV1584-DMS (MDD), 2014 WL 585868, at *4 (S.D. Cal. Feb. 13, 2014) ("The definitional, typically boilerplate, section of requests for production cannot be used to expand the scope of a request for production into an interrogatory.").

C. Draft Well-Tailored, Proportional Requests

The same principles that apply to the definitions and instructions apply to the requests themselves. The requesting party should draft well-tailored document requests that identify the discrete time period at issue in connection with the particular request and the items or category of items sought.[93] Requests should also abide by Rule 26(b)'s admonition that discovery should be "proportional to the needs of the case."[94] The following principles may be considered when drafting requests.

1. Request Specific, Identifiable, or Discrete Documents

Counsel should attempt to draft requests for specific documents important to the claims or defenses that are readily identifiable. Consider categories of documents that for many organizations or individuals may be kept in a discrete location and may be relatively easy to collect (absent unique circumstances) such as:

- account statements related to the plaintiff's account in a case involving financial transactions;

---

93. The party drafting a document request has the burden of fashioning the request appropriately. *See* Washington v. Thurgood Marshall Acad., 232 F.R.D. 6, 10 (D.D.C. 2005). "Standard" requests are disfavored. *See, e.g.*, Michael Kors, L.L.C. v. Ye, No. 1:18-CV-2684 (KHP), 2019 WL 1517552, at *3 (S.D.N.Y. Apr. 8, 2019) ("The 2015 amendments to the Rules were designed to stop counsel from relying on standard, overbroad requests and to also require tailoring based on the particular issues and circumstances in the case.").

94. *See* FED. R. CIV. P. 34 (limiting discoverable documents to those "within the scope of Rule 26(b)"); *see also* Hon. Craig B. Shaffer, *The "Burdens" of Applying Proportionality*, 16 SEDONA CONF. J. 55 (2015) ("Claims of ignorance should not absolve an attorney of his or her responsibility to pursue discovery that is proportional to the needs of the case nor excuse discovery requests that bear more resemblance to unguided missiles than thoughtful efforts to obtain truly relevant information.").

- a personnel file related to an individual in an employment case;
- statements of work, the final contract, and invoices related to a contract dispute; or
- a particular policy in a discrete time period that relates to the claim.

Responding parties may be able to quickly produce documents responsive to specific, targeted requests. Consider making the request as simple and targeted as possible, such as "produce all board minutes from 2012 related to the Acme contract," or "produce the original design specifications for the [relevant component] in the [relevant product]."

Also, note that requests beginning with the "any and all" preamble usually draw objections and delay production, but such requests may be narrowed depending on the needs of the case. For example, a request for "any and all documents related to policies and procedures" would appear to call for all communications around the drafting and implementing of the policies and procedures, which may be unnecessary where the requesting party simply needs a specific policy or procedure that was applied to the transaction giving rise to a claim or defense.

In addition, when requesting email or other electronic communications, counsel should narrow requests by, for example, seeking only communications between certain relevant individuals and during discrete relevant time periods and about specific topics. Specific topics can guide the responding party in developing appropriate search parameters and methodologies. The volume of emails and communications sent though other mediums has exponentially increased over recent years. Even requests for a small number of custodians' communications can require substantial time and cost to collect and review, particularly if the request spans a number of years.

2. "Sufficient to Show" Requests and Interrogatories in Lieu of Requests

Counsel should consider "sufficient to show" requests when appropriate, as they are often less objectionable than those requesting "any and all" documents.[95] Sufficient-to-show requests seek documents on a topic about which counsel needs information, but where counsel does not need the responding party to find and produce *every* document that contains or relates to that information. Sufficient-to-show requests can be helpful for producing necessary, noncontroversial documents to confirm a presumption in the case. An initial round of sufficient-to-show requests may be useful in framing iterative discovery requests. Sufficient-to-show phrasing may prompt a quicker production of relevant information because the producing party may be able to identify and produce what is sufficient to show the specific request without searching all ESI on the topic. In order to maintain the utility of sufficient-to-show requests, responses to these requests should be an unbiased and representative selection of documents and not be used as an opportunity to produce only documents favorable to one position while withholding unfavorable documents.

For example:

95. Vangelakos v. Wells Fargo Bank, No. 13-cv-06574-PKC, at *1–2 (S.D.N.Y. Feb. 4, 2014), ECF No. 21. In *Vangelakos*, the court held in a wage and hour case, that "Plaintiffs' request for all emails to or from the employee during the course of their employment is hopelessly overbroad. It would likely pick up appeals for corporate sponsored charities and company personnel news. More importantly, it is not necessary to reconstruct the worklife of each plaintiff on each day of employment in order to prosecute or defend a FLSA case. The Federal Rules of Civil Procedure counsel in favor of proportionality." *Id*. The court went on to state that it did not foreclose the possibility that a limited test period of 30 days, for example, might be appropriate for some type of email search. *Id*.

- Where information about the locations where the responding party did business is relevant and proportional, a request for information "sufficient to show all locations where Company A did business in 2012 to 2015" would be more appropriate than a request for "all information that reflects or relates to the locations where Company A did business."
- Where organizational charts and other information that would establish the responding party's structure are relevant, requests seeking information "sufficient to show" the organizational structure as it relates to the case would be an effective way to obtain the evidence needed in a proportional way. Note how such a request does not seek evidence about the organization globally, nor does it ask for all documents reflecting the organization's structure. Specificity is key here. For example, in a breach-of-contract case, requests for materials sufficient to show the individuals involved in the formation, execution, and breach of the contract and to whom they reported could be reasonable and specific.
- Where information about the development of a particular product may be relevant, such as in a trademark infringement case or certain types of product liability cases, requests seeking information "sufficient to show" the design of the product or a particular component at issue may be an effective way to obtain the evidence needed to establish a claim or defense. This phrasing may avoid or minimize disputes about irrelevant competitive or other information that may be

prompted by a request for "all documents" about the product.

- In a case related to reasonable accommodation, consider whether it would be appropriate to request information sufficient to show the nature of accommodations provided to potential comparator employees without requesting "all" information related to those requests. This would allow the requesting party to see what other types of accommodations an employer has provided without producing non-party medical information.

Sufficient-to-show document requests may not be reasonably particular when seeking information to satisfy a legal element of a claim, however. For example, a request for documents "sufficient to show that defendant breached the standard of care" in a professional malpractice lawsuit is not sufficiently particular, as it seeks documents to prove a legal conclusion. It may also invade attorney work product, as seeking discovery from an opponent to prove legal conclusions necessarily requires application and disclosure of attorney mental impressions.

In some cases, an interrogatory may be a more efficient way to obtain the needed information. For example, an interrogatory requiring identification of the locations where the responding party did business may be more straightforward than a sufficient-to-show request. Alternatively, instead of requesting "all ESI that relates to the Acme Widgets account," consider an interrogatory that asks the responding party to list all products sold to Acme Widgets, the dates those products were sold, and prices at which the products were sold. Note that the Federal Rules of Civil Procedure pose limits on the number of

interrogatories propounded; however, there is no such limit on document requests.

"Any and all" requests may still be appropriate for documents that go to the heart of the claims or defenses and for which the full breadth of responsive materials may itself be instructive. To illustrate, in an antitrust case, every communication among competitors about supply or pricing of the relevant products may be critical to proving the existence of a conspiracy. "Documents sufficient to show" under these circumstances may be insufficient. "Any and all" requests may also be appropriate when the requests seek only a limited, knowable number of the documents. In a slip-and-fall case, a party may request all surveillance footage of the incident. The key is to use "any and all" requests sparingly and appropriately.

3. Limit Requests to Specific Custodians

Identifying specific custodians or locations may further the goal of particularity in requests. Requests for information about relevant communications associated with particular custodians may provide greater specificity when used in conjunction with requests for relevant content, as opposed to requests for "any and all" content or communications to/from/cc/bcc "any and all" custodians. For example, in a breach-of-contract case, requests seeking all communications authored by the contract negotiator about the contract during the relevant time period may provide adequate specificity because the request includes limitations as to custodian, time period, and relevant content. In circumstances where there is a high degree of information asymmetry between the parties, limiting requests to certain custodians may require sharing basic information regarding relevant custodians and departments in order to appropriately narrow the requests. If a requesting party cannot see a way to narrow an "any and all" request, counsel should consider

conferring with opposing counsel and preparing a list of questions that would supply information useful to narrowing the request.

4. Include a Temporal Scope in the Request

At its core, the "reasonable particularity" concept requires identification of documents by subject matter and time frame.[96] That is the essence of the requirement. Therefore, all requests should, at a minimum, identify a temporal limitation and describe with particularity the subject matter of the documents sought. The specificity with which the temporal scope can be defined, of course, depends upon the specific facts and circumstances of a case.[97] Opening cooperative dialogue with the responding party about these issues may help counsel draft the targeted requests contemplated by the Rules.

5. Requests Tied to Specific Allegations or Arguments

Consider using factual contentions made by the responding party (in the answer or other response to the complaint or in a deposition) to define the limits of a request. Where a responding party has asserted certain facts, requests targeted at testing the veracity of such assertions may be appropriate.

96. *See supra* Section II.A.

97. *See, e.g.*, Carlson v. Sam's West, Inc., No. 2:17-cv-02882-MMD-GWF, 2018 WL 4094856, at *2 (D. Nev. Aug. 28, 2018) (collecting cases that discuss "reasonable particularity" in the Rule 34 context to address the similar language in Rule 30(b)(6)).

V. CONCLUSION

Well-crafted Rule 34 requests are important tools in securing "the just, speedy, and inexpensive determination of every action and proceeding" as required by Rule 1. Drafting well-crafted Rule 34 requests requires counsel to think about the needs of the case. In most cases, this means avoiding robotic reliance on forms or templates, particularly template definitions and instructions that do not apply to the case. Instead, counsel should use available resources to make the requests reasonably particular and applicable to counsel's case. Regardless of the case, meeting and conferring in good faith can be an essential resource. Depending on the case, other resources may include delivering early Rule 34 requests, staging discovery, setting reasonable time frames for requests, limiting requests to specific custodians or locations, requesting specific documents or information sufficient to establish a particular factual issue, using requests for "any and all documents" thoughtfully, and thinking at the outset how to defend each request in the event of a challenge.

The early investment of time in crafting thoughtful, reasonably particularized Rule 34 requests, and meaningfully meeting and conferring where appropriate, is likely to reduce delay in conducting discovery and objections. Where objections are made, these techniques are likely to assist the requesting party in overcoming them through informal conferences and formal motion practice. The ideas presented in this *Primer* will help in preparing such well-crafted requests, which will promote efficiency and cost savings associated with discovery in litigation.

THE SEDONA CONFERENCE COMMENTARY ON THE NEED FOR GUIDANCE AND UNIFORMITY IN FILING ESI AND RECORDS UNDER SEAL

A Project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)

Author:

The Sedona Conference

Drafting Team Leaders:

Bethany Caracuzzo
Tony Petruzzi
Jodi Munn Schebel

Drafting Team:

Zachary Caplan
Karen Mitchell
Maria Salacuse
Jeff Schaefer

Judicial Advisors:

Hon. Maria A. Audero
Hon. Cathy Bissoon
Hon. Timothy S. Driscoll

Steering Committee Liaisons:

Ross Gotler
Heather Kolasinsky
Timothy Opsitnick
Hon. Andrew J. Peck (ret.)
Martin T. Tully

Staff editor:

David Lumia

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

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, *Commentary on the Need for Guidance and Uniformity in Filing ESI and Records Under Seal*, 23 SEDONA CONF. J. 379 (2022).

PREFACE

Welcome to the final, February 2022 version of The Sedona Conference *Commentary on the Need for Guidance and Uniformity in Filing ESI and Records Under Seal ("Commentary")*, a project of The Sedona Conference Working Group 1 on Electronic Document Retention and Production (WG1). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The intent of this *Commentary* is to minimize the burden on litigants and courts created by the lack of uniformity in United States district court procedures for sealing confidential documents and electronically stored information (ESI). The *Commentary* offers a Proposed Model Rule designed both to bring uniformity to the process of filing under seal and to create a fair and efficient method to deal with the sealing and redacting of ESI, so that the parties can focus on the litigation while conserving the resources of the court. The Proposed Model Rule does not provide any guidelines or guidance for what ESI is properly sealed or redacted; it only provides a procedure for doing so.

The *Commentary* was a topic of dialogue at the Working Group 1 2020 Annual Meeting and 2021 Midyear Meeting, and an initial draft was distributed for member comment in 2021. The draft was revised based on member comment and published for public comment in December 2021. After sufficient opportunity for public comment, the *Commentary* is now published in its final, February 2022 version.

On behalf of The Sedona Conference, I thank drafting team leaders Bethany Caracuzzo, Tony Petruzzi, and Jodi Munn Schebel for their leadership and commitment to the project. I

also recognize and thank drafting team members Zachary Caplan, Karen Mitchell, Maria Salacuse, and Jeff Schaefer for their dedication and contributions, and Steering Committee liaisons Ross Gotler, Heather Kolasinsky, Timothy Opsitnick, the Hon. Andrew Peck, and Martin Tully for their guidance and input. I also wish to recognize the Hon. Maria Audero, the Hon. Cathy Bissoon, and the Hon. Timothy Driscoll for their contributions as Judicial Advisors.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; patent remedies and damages; patent litigation best practices; trade secrets; data security and privacy liability; and other "tipping point" issues in the law. 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. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
February 2022

TABLE OF CONTENTS

I. INTRODUCTION

As any practitioner in federal court knows, there is a lack of uniformity as to the process for sealing confidential documents and electronically stored information (ESI). Federal Rule of Civil Procedure 5.2 provides concrete and repeatable rules for sealing personal information, including social security, tax-ID and financial account numbers, as well as birth dates and the names of minors, but guidance from the rules as to sealing stops there. If a party wants to use a produced confidential document in support of a motion for summary disposition, for example, the process it must follow is almost entirely governed by local rules. And those rules are so varied that not only do they differ from district to district,[1] but also differ between districts within the same state.[2]

Frequently, those rules place the burden to seal a document on the party that did not designate the document as containing confidential information, and in many cases disagrees with that designation. Under traditional sealing rules, the filing party must move to seal confidential documents appended to or referenced in a motion. However, if the filing party did not produce the confidential documents, the filing party has no knowledge as to the reason(s) why any individual confidential document was designated as such by the producing party.

1. For example, in the Northern District of New York, all documents sought to be sealed must be sent to the court for in camera review in .pdf format through an email to the assigned judge, and served on all counsel. See N.D.N.Y. L.R. 83.13(6). However, in the Central District of California, sealed documents must be filed electronically. See C.D. Cal. L.R. 79-5.

2. An order to seal in the Western District of Texas lasts unless otherwise directed by the Court. *See* W.D. Tex. L.R. 5.2(d). However, in the Northern District of Texas, an order to seal paper documents is deemed unsealed 60 days after final disposition of the case, unless a party seeking to maintain the order to seal files a motion for relief before expiration of the time period. *See* N.D. Tex. L.R. 79.4.

Thus, not only does the filing party lack foundation upon which to base a motion to seal, it may not even agree that the confidential documents deserve to be sealed. This results in an impracticable situation in which, by application of local sealing rules, the filing party must file a motion to seal documents that it may actually oppose. As a result, the filed motion to seal is oftentimes perfunctory and lacking in meaningful content. So that the court can properly weigh whether the confidential documents meet the requirements to be sealed,[3] this *Commentary* posits that it should be the designating party's burden to file a declaration in support of sealing, because the designating party is uniquely situated and appropriately motivated to describe the nature and basis of each confidential document. Only upon such proper foundation can the court determine whether the documents or information at issue should be sealed from public view.

To rectify this problem, this *Commentary* proposes the use of a Notice of Proposed Sealed Record, which is filed with the underlying motion, pleading, or response, and identifies the confidential documents referenced in or appended to that motion, pleading, or response. The Notice, proposed in this *Commentary* to be a standardized and simple form for consistency and

3. The substantive standard to be used by a court in considering whether a document should be sealed in whole or in part is an entirely different matter from the procedure addressed by the Proposed Model Rule and is not addressed by this *Commentary* or the Proposed Model Rule, which is procedural only. Applicable standards include the common law right of access, the right of access under the First Amendment, and Federal Rule of Civil Procedure 26(c)(1)(G), which permits a party to seek protection, on a showing of good cause, from "annoyance, embarrassment, oppression, or undue burden or expense" as to "requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way[.]" For ease of reference and to provide background on the applicable standard for sealing and the split among the federal circuits as to the proper standard to be applied, an Appendix Case Law Summary is attached to this *Commentary*.

efficiency, then triggers the obligation of the designating party to file a properly supported motion to seal. This process change not only eases the burden on the filing party, but also places the burden to seal on the proper party—the party that produced the documents with a confidential designation. The Proposed Model Rule also addresses other inconsistencies and differences between the local sealing rules, including setting a uniform and reasonable time frame to file a motion to seal, proper notice to be provided to non-parties whose confidential documents are subject to a Notice of Proposed Sealed Record, and how sealed and redacted records are to be filed by the parties and disposed of by the court. The proposed Notice form also aids courts, litigators, non-parties, and the public by using a clear and consistent docketing entry signaling that a motion to seal has been filed.

These changes, like the others proposed in this *Commentary* and its Proposed Model Rule, are designed to not only bring uniformity to the process of filing documents and ESI under seal, but to be a fair and efficient method to deal with the sealing and redacting of ESI and documents so that the parties can focus on the litigation while conserving the resources of the court. To effect these goals, this *Commentary*: (1) recommends a consistent process for filing ESI and documents under seal, considering the attendant burdens for sealing on parties, non-parties, and the court; and (2) provides guidance and best practices to practitioners on ESI and document sealing, including the steps required to do so and potential pitfalls to avoid in the process.

In addition to this Introduction, this *Commentary* includes two other sections:

- Section II is the Proposed Model Rule, with Proposed Notice form;
- Section III is an annotated version of the Proposed Model Rule containing practice tips for

> complying with the Proposed Model Rule, discussion of the factors considered by the drafting team and inconsistencies presented by the multiple differing local federal rules, and a process flowchart illustrating the practical application of the Proposed Model Rule.

Finally, the Appendix includes a circuit-by-circuit case law summary analyzing federal law on the standards for sealing of ESI and documents, with attachments. Attachment A depicts, in a chart format, whether and how each federal circuit defines a "judicial record," and Attachment B identifies whether a public right of access exists for nondispositive motions in each federal circuit.

By providing a uniform process, including a single set of rules for sealing documents in civil litigation and a standardized form for providing notice of the filing of sealed documents, this Proposed Model Rule, if enacted, should ease the burden on litigants and the court alike, and lead to a more equitable process for all.

II. PROPOSED UNIFORM MODEL RULE FOR THE SEALING AND REDACTING OF INFORMATION FILED WITH A FEDERAL COURT WITH PROPOSED FORM OF NOTICE

Model Rule: Procedures for the Sealing and Redaction of Records in a Federal Civil Case

1.0 Definitions

As used in this Rule:

(A) Conditionally Sealed Period. The Conditionally Sealed Period is the time period during which a Record is temporarily sealed because it is identified in a Notice of Proposed Sealed Record, but has not yet been sealed pursuant to court order.

(B) Confidential Information. Confidential Information is information the Filing Party or Designating Party contends is confidential or proprietary in a Notice of Proposed Sealed Record or a motion to seal, including information that has been designated as confidential or proprietary under a protective order or nondisclosure agreement, or information otherwise entitled to protection from disclosure under statute, rule, order, or other legal authority.

(C) Court Record. The Court Record refers to the full collection of pleadings, motions, orders, and exhibits that make up a case file.

(D) Designating Party. The Designating Party is the person or entity that designated the Confidential Information at issue under this Rule. The Designating Party may be a non-party to the case and may also be the Filing Party for purposes of this Rule.

(E) Filing Party. The Filing Party is the party seeking to file Confidential Information.

(F) Presumptively Protected Information. A Record may contain Presumptively Protected Information if it includes any of the following:

(1) Personally Identifiable Information (PII) refers to information that can, either alone or when combined with other personal or identifying information, be used to distinguish or trace an individual's identity, such as social security number, or biometric records, or information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, or father's middle name;

(2) Information defined as Protected Individually Identifiable Health Information (PHI) by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and including information protected by comparable federal, state, or local laws, regulations, or rules governing healthcare information privacy;

(3) Information otherwise protected from disclosure by federal, state, or local laws, regulations, or rules governing data privacy;

(4) Information not otherwise covered by Federal Rule of Civil Procedure 5.2 ("Rule 5.2"), such as passport numbers, taxpayer ID numbers, military ID numbers, driver's license numbers; other national, state, or local government issued identification, license, or permit numbers; nonfinancial customer account numbers; internet or website user names, login IDs, or passwords; personal email addresses; personal telephone numbers; personal device internet protocol (IP) addresses; residence addresses; and personal geolocation data (except if such

information must be publicly disclosed by rule or order, *e.g.*, residence address on initial pleading, docket form, summons, subpoena, or substantively in a given case).

(G) Proposed Sealed Record(s). A Proposed Sealed Record is a Record that is temporarily sealed or redacted during the Conditionally Sealed Period by virtue of its attachment to a Notice of Proposed Sealed Record or motion to seal.

(H) Record. Unless the context indicates otherwise, Record means all or a portion of any document, pleading, motion, paper, exhibit, transcript, image, electronic file, or other written, printed, or electronic matter filed or lodged with the court, by electronic means or otherwise.

(I) Redacted Record. A Redacted Record is a Record that, by court order, contains a specific subset of information that is not open to inspection by the public, but the Record itself is not entirely sealed.

(J) Sealed Record. A Sealed Record is a Record that by court order is not open to inspection by the public or is temporarily sealed pursuant to the Conditionally Sealed Period.

2.0 Sealing Presumptively Protected Information

(A) No prior Court approval required.

A Filing Party who seeks to file Presumptively Protected Information identified in Rule 5.2 shall follow its requirements. For all other Presumptively Protected Information as defined by Model Rule 1.0(F), the Filing Party may redact such information without prior court approval where the extent of the redaction(s) is no greater than required to protect the disclosure of such information. Where other content in a Record supports or requires filing under seal,

the provisions of Model Rule 3.0 apply, notwithstanding any redactions made under this section.

(B) No requirement to redact received materials.

A Filing Party receiving unredacted Records from a Designating Party is not required by this section to apply redactions to the Designating Party's Records before filing. This provision does not supersede any court order (such as a protective order or ESI order), law, regulation, or rule that imposes an affirmative requirement on a receiving party to redact information prior to filing, including Rule 5.2.

(C) No requirement to defend Designating Party's redactions.

A Filing Party receiving redacted Records from a Designating Party is not required to defend the appropriateness of redactions made by a Designating Party under this section in order to file them in the form received, after providing the Notice set forth in Model Rule 3.0(C). This provision does not preclude a receiving party from objecting to or challenging redactions by a Designating Party.

(D) Redactions to be no more extensive than required.

Redactions to prevent unauthorized public disclosure of information described in Model Rule 1.0(F) should be no more extensive than required to maintain the confidentiality of the Presumptively Protected Information, and should not, where feasible, obscure the type of information being redacted, if the nature of the type of information is indicated on the original document; *for example*, "D.O.B. ____".

(E) Redactions to be textual where feasible.

To apprise viewers of the bases for redactions, where the technology used to redact provides for textual redactions

(as opposed to blackbox or whitebox redaction), textual redactions that characterize the redactions should be used (e.g., "PHI/PII Redacted," or "Personal Protected Information Redacted").

3.0 All Other Sealing

(A) Court approval required.

A Record must not be filed under seal or redacted without a court order, except in connection with a Notice of Proposed Sealed Record, or if the Record contains Presumptively Protected Information governed by Model Rule 2.0. A Record filed under seal in connection with a Notice of Proposed Sealed Record will be temporarily sealed unless and until an order disposing the motion to seal is entered, *e.g.*, the "Conditionally Sealed Period." Thereafter, the Record remains sealed unless determined otherwise by an order of the court. See Model Rules 1.0(A), 3.0(F), and 4.0.

(B) CM/ECF filing requirement.

(1) Unless otherwise ordered by the court, any Record to be filed under seal, Notice of Proposed Sealed Record, or motion to seal must be filed electronically with restricted access using the court's Case Management/Electronic Case Filing (CM/ECF) System. Notwithstanding this requirement, a Filing Party who is not represented by an attorney (*i.e.*, is "pro se") must not file electronically unless the pro se is approved to become a CM/ECF user in that case pursuant to local rules or court order. If a pro se party is not an approved CM/ECF user, the pro se must file such documents in paper form, and the Clerk of Court will perform the necessary filing steps in the CM/ECF system.

(2) Proposed Sealed Records are to be filed only with the underlying motion, pleading, or response,

and each such Record shall be filed separately so that each document is assigned its own ECF docket number (*e.g.*, ECF No. 2, or ECF No. 2-2). The Proposed Sealed Record(s) must be filed as separate docket entries in both sealed and unsealed and redacted and unredacted forms. Any Filing Party must file a Notice of Proposed Sealed Record pursuant to Model Rule 3.0(C).

(3) Nonpublic Filing of Proposed Sealed or Redacted Records. An unsealed or unredacted copy of each Proposed Sealed or Redacted Record must be filed concurrently with the motion, pleading, or response to which the Proposed Sealed or Redacted Record(s) are referenced or attached, using CM/ECF restricted viewing. All Records filed under seal or in unredacted form must state "FILED CONDITIONALLY UNDER SEAL" at the top of the Record or in such a place so as not to obscure the content of the document.

(4) Publicly Filed Versions of Proposed Sealed and Redacted Records. Redacted Records must be filed in redacted form in the public record. A Record to be sealed in its entirety must be filed in the public record by a placeholder slip sheet stating "DOCUMENT FILED UNDER SEAL." Each Proposed Sealed Record that is an attachment to a filing must be numbered (*e.g.*, as "Sealed Exhibit Number ___" and "Redacted Exhibit Number ___").

(5) Filing a document under seal does not exempt the filer from the service requirements imposed by federal statutes, rules, or regulations or by a court's local rules. E-service on parties in sealed or unredacted forms will be accomplished through the

CM/ECF system, where available. If CM/ECF service is unavailable for such Records, a Filing Party who is an approved CM/ECF user must accomplish service same day as otherwise required by the Federal Rules of Civil Procedure, Federal Rules of Criminal Procedure, and Local Rules. Service on a pro se party or non-party who has not been previously approved to be a CM/ECF user in the case must be made in accordance with Federal Rule of Civil Procedure 5.

(6) The motion to seal and its supporting documents, identified below in Model Rule 3.0(D), must not be filed under seal or with redactions unless the motion cannot be drafted in a manner that protects the Confidential Information from disclosure.

(7) Any order disposing of a motion to seal should be publicly filed.

(C) Notice of Proposed Sealed Record.

(1) Filing of Notice of Proposed Sealed Record. If a Filing Party intends to file a motion, pleading, or response that references or appends Confidential Information, it must file a Notice of Proposed Sealed Record. A Filing Party must file a Notice of Proposed Sealed Record even if it is the Designating Party.

(2) Content of Notice of Proposed Sealed Record. The Notice of Proposed Sealed Record must identify each Proposed Sealed or Redacted Record or generally identify the Confidential Information that was redacted from each Proposed Sealed or Redacted Record, without disclosing Confidential Information, and identify the corresponding Designating Party. Each Proposed Sealed or Redacted Record shall be referred to the ECF docket

number from the motion, pleading, or response to which the Proposed Sealed Records are referenced or attached.

(3) Notice Where Records Previously Sealed or Redacted by Court Order. If Records subject to the Notice of Proposed Sealed Record were previously sealed or redacted by court order in the same action, the Filing Party must file a Notice of Proposed Sealed Record in compliance with this section and identify the prior order by ECF docket number and date. A new motion to seal is not required if the court previously ordered the Record sealed or redacted.

(4) Timing of Notice of Proposed Sealed Record. A Notice of Proposed Sealed Record must be filed immediately after any motion, pleading, or response to which the Proposed Sealed or Redacted Records are referenced or attached (*e.g.*, a motion to compel, a motion for summary judgment, or a motion in limine).

(5) Notice to Non-Party Designating Parties. If Records subject to the Notice of Proposed Sealed Record were produced by a Designating Party that is a non-party to the litigation, the Filing Party filing the Notice of Proposed Sealed Record must provide notice of the filing to the non-party in accordance with Rule 3.0(B)(5).

(D) Motion to Seal.

(1) Motion to Seal. If a Designating Party whose Record(s) are the subject of a Notice of Proposed Sealed Record seeks to maintain such Records under Seal, the Designating Party must file a motion to seal. A Filing Party who is the Designating Party must file

and serve the motion to seal in compliance with this Rule.

(2) Memorandum. The motion to seal must include a nonconfidential memorandum in support that complies with Model Rule 3.0(B)(6) describing: (a) each Record(s) to be sealed or redacted; (b) the basis for the request; and (c) how each Record(s) to be sealed or redacted meets applicable standards for sealing.

(3) Declaration in Support. The motion to seal must include a nonconfidential declaration in support setting forth the legal basis for filing each Record under seal or in redacted form, and such Records should not be refiled, but should be identified by their ECF docket numbers from the motion, pleading, or response to which the Proposed Sealed Record(s) is referenced or attached (*e.g.*, ECF No. 2 or ECF No. 2-2).

(4) Timing of Motion to Seal. A Designating Party must file its motion to seal and supporting declaration within the time frame set for the filing of any responsive pleading to the motion that references or appends a Designating Party's Confidential Information, unless otherwise ordered by the court. If a responsive pleading is not permitted, the motion to seal and supporting declaration must be filed within seven (7) court days of service of the Notice of Proposed Sealed Record.

(5) Failure to Timely Move to Seal. If the Designating Party does not timely file its motion to seal in accordance with this Rule, the Designating Party waives its right to maintain that the Records contain Confidential Information.

(E) Proposed Order. A proposed order must be filed and served with the motion to seal.

(F) Disposition of Proposed Sealed Records.

(1) If the Designating Party fails to timely file a motion to seal after receiving Notice pursuant to Model Rule 3.0(C) above, the Filing Party must publicly file the Confidential Information in unredacted and unsealed form within seven (7) court days of the expired motion to seal deadline.

(2) If the court grants the motion to seal, the Proposed Sealed Record will be deemed filed as of the date of the filing of the Notice of Proposed Sealed Record unless otherwise directed by the court.

(3) If the court denies the motion to seal, the Filing Party shall publicly file the Confidential Information in unredacted and unsealed form within seven (7) court days of the order denying the motion to seal, or take other action as ordered by the court.

4.0 Disposition of Sealed and Redacted Records at the Conclusion of the Case.

Unless otherwise ordered by the Court, a Sealed or Redacted Record will remain sealed or redacted after final disposition of the case. Anyone seeking to unseal or unredact a Record may petition the court by motion. The motion must be served upon all parties in the case and upon any Designating Party that is a non-party in accordance with the service requirements in this Rule.

FORM NOTICE OF PROPOSED SEALED RECORD

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF

_____ *
Plaintiff, *

v. **Case No.** _____ *

_____ *
Defendant. *

NOTICE OF PROPOSED SEALED RECORD

The undersigned hereby provide Notice of a Proposed Sealed Record, setting forth below the ECF Number(s) of the document(s) to be sealed, the identity of the designating party or non-party, whether an objection to sealing is anticipated, and whether a prior sealing Order exists.

ECF No.	Designating Party	Objection Anticipated	Prior ECF No.	Prior Order Date
		--Select--		
		--Select--		
		--Select--		
		--Select--		
		--Select--		
		--Select--		
		--Select--		
		--Select--		
		--Select--		
		--Select--		

If no prior Order exists, proposed reason for redacting or sealing:

I hereby certify that on this date I electronically filed this Notice and the documents identified above with the Clerk of the Court using the ECF system which sent notification of such filing to all counsel of record, and that for any non-parties, I will serve copies of this Notice and the documents identified above in conformance with Fed. R. Civ. P. 5 and applicable Local Rules.

_____ _____

Date

Signature

Party Represented

Printed Name and Bar Number

Address

Email Address

Telephone Number

Fax Number

PRINT

III. ANNOTATED PROPOSED UNIFORM MODEL RULE FOR THE SEALING AND REDACTING OF INFORMATION FILED WITH A FEDERAL COURT

Model Rule: Procedures for the Sealing and Redaction of Records in a Federal Civil Case

1.0 Definitions

As used in this Rule:

(A) Conditionally Sealed Period. The Conditionally Sealed Period is the time period during which a Record is temporarily sealed because it is identified in a Notice of Proposed Sealed Record, but has not yet been sealed pursuant to court order.

(B) Confidential Information. Confidential Information is information the Filing Party or Designating Party contends is confidential or proprietary in a Notice of Proposed Sealed Record or a motion to seal, including information that has been designated as confidential or proprietary under a protective order or nondisclosure agreement, or information otherwise entitled to protection from disclosure under statute, rule, order, or other legal authority.

❖ *COMMENT*

Standing alone, the fact that a Record contains Confidential Information is not enough to justify sealing or redaction, nor is the existence of a Protective Order permitting "Confidential" or similar designations.[4]

4. The federal courts have long recognized different standards for maintaining the confidentiality of documents that are exchanged in discovery versus documents filed with the court. For example, the Third Circuit recently reiterated that once documents are filed with a court "there is a presumptive

> Records submitted under seal or in redacted form pursuant to this Model Rule cannot remain under seal without a court order determining such sealing or redacting is proper, except for Presumptively Protected Information (See definition at 1.0(F) and Model Rule 2.0) or as required by Federal Rules of Civil Procedure 5.2.[5]
>
> The proposed Model Rule does not seek to set forth any guideline or guidance as to what information is properly sealed or redacted; it only provides a procedure for doing so.
>
> When this Model Rule refers to redacted documents, it means redactions for purpose of public filing, not redactions that already exist on the document as part of production (e.g., redactions for privilege).

right of public access to pretrial motions of a non-discovery nature, whether preliminary or dispositive, and the material filed in connection therewith." *In re* Avandia Mktg. Sales Practices & Prod. Liab. Litig., 924 F.3d 662, 672 (3d Cir. 2019); *see also*, *for example*, Lugosch v. Pyramid Co. of Onondaga, 435 F.3d 110, 119 (2d Cir. 2006). Parties and attorneys practicing in federal courts—particularly in courts in the Third Circuit—should be aware of these decisions encouraging increased judicial scrutiny of proposed under seal filings.

5. The definition of Presumptively Protected Information under the Proposed Uniform Model Rule is broader than that covered in Federal Rule of Civil Procedure 5.2. Note, however, that some courts will not allow filing of redacted materials except to the extent permitted by the Federal Rules of Civil Procedure. *See, for example*, D.N.J. Electronic Case Filing Policies and Procedures (As Amended April 3, 2014), Section 10, https://www.njd.uscourts.gov/sites/njd/files/PoliciesandProcedures2014.pdf ("Unless otherwise provided by federal law, nothing may be filed under seal unless an existing order so provides or Local Civil Rule 5.3 is complied with.").

(C) Court Record. The Court Record refers to the full collection of pleadings, motions, orders, and exhibits that make up a case file.

(D) Designating Party. The Designating Party is the person or entity that designated the Confidential Information at issue under this Rule. The Designating Party may be a non-party to the case and may also be the Filing Party for purposes of this Rule.

(E) Filing Party. The Filing Party is the party seeking to file Confidential Information.

(F) Presumptively Protected Information. A Record may contain Presumptively Protected Information if it includes any of the following:

> **(1)** Personally Identifiable Information (PII) refers to information that can, either alone or when combined with other personal or identifying information, be used to distinguish or trace an individual's identity, such as social security number, or biometric records, or information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, or father's middle name;
>
> **(2)** Information defined as Protected Individually Identifiable Health Information (PHI) by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and including information protected by comparable federal, state, or local laws, regulations, or rules governing healthcare information privacy;
>
> **(3)** Information otherwise protected from disclosure by federal, state, or local laws, regulations, or rules governing data privacy;

(4) Information not otherwise covered by Federal Rule of Civil Procedure 5.2 ("Rule 5.2"), such as passport numbers, taxpayer ID numbers, military ID numbers, drivers' license numbers; other national, state, or local government issued identification, license, or permit numbers; nonfinancial customer account numbers; internet or website user names, login IDs, or passwords; personal email addresses; personal telephone numbers; personal device internet protocol (IP) addresses; residence addresses; and personal geolocation data (except if such information must be publicly disclosed by rule or order, *e.g.*, residence address on initial pleading, docket form, summons, subpoena, or substantively in a given case).

❖ *COMMENT*

This new definition and the provisions that follow in Section 2.0 for redaction of Presumptively Protected Information are intended to augment Federal Rule of Civil Procedure 5.2 and provide streamlined protection from disclosure for a broader group of materials than currently are set forth in Rule 5.2. The definition covers information that is defined elsewhere, such as PII and PHI.

(G) Proposed Sealed Record(s). A Proposed Sealed Record is a Record that is temporarily sealed or redacted during the Conditionally Sealed Period by virtue of its attachment to a Notice of Proposed Sealed Record or motion to seal.

(H) Record.[6] Unless the context indicates otherwise, Record means all or a portion of any document, pleading, motion, paper, exhibit, transcript, image, electronic file, or other written, printed, or electronic matter filed or lodged with the court, by electronic means or otherwise.

(I) Redacted Record. A Redacted Record is a Record that, by court order, contains a specific subset of information that is not open to inspection by the public, but the Record itself is not entirely sealed.

(J) Sealed Record. A Sealed Record is a Record that by court order is not open to inspection by the public or is temporarily sealed pursuant to the Conditionally Sealed Period.

2.0 Sealing Presumptively Protected Information

(A) No prior Court approval required.

A Filing Party who seeks to file Presumptively Protected Information identified in Rule 5.2 shall follow its requirements. For all other Presumptively Protected Information as defined by Model Rule 1.0(F), the Filing Party may redact such information without prior court approval where the extent of the redaction(s) is no greater than required to protect the disclosure of such information. Where other content in a Record supports or requires filing under seal, the provisions of Model Rule 3.0 apply, notwithstanding any redactions made under this section.

---

6. In considering the proper term for this document, this *Commentary* looked to the terms used by the varying circuits, which include "record," "judicial record," "document," "judicial document," "item," or "material." This document is to be distinguished from a document that becomes a part of the court file in a case (*see* 1.0(C)), but instead is meant to identify the document sought to be sealed or redacted pursuant to this Rule.

❖ *COMMENT*

The Model Rule proposes that a streamlined process of redaction is appropriate only to protect Presumptively Protected Information, and therefore does not require the procedure set forth in Model Rule 3.0 for filing Presumptively Protected Information under seal. Although the proposed Model Rule does not require prior court approval for the filing of Presumptively Protected Information, it does not preclude a party from challenging the filing or a non-party from intervening under Federal Rule of Civil Procedure 24(b) to challenge the sealing or redacting of any Record, including Presumptively Protected Information.

(B) No requirement to redact received materials.

A Filing Party receiving unredacted Records from a Designating Party is not required by this section to apply redactions to the Designating Party's Records before filing. This provision does not supersede any court order (such as a protective order or ESI order), law, regulation, or rule that imposes an affirmative requirement on a receiving party to redact information prior to filing, including Rule 5.2.

❖ *COMMENT*

Unless redaction is required by Federal Rule of Civil Procedure 5.2, the Model Rule does not obligate a Filing Party to redact Presumptively Protected Information when it has received documents or ESI in an unredacted form from the Designating Party. In that case, the party or entity producing materials that contain Presumptively

Protected Information should bear the burden of protecting such information from disclosure. However, the Model Rule does not supersede any legal requirement that imposes a duty to protect any such information from disclosure.

(C) No requirement to defend Designating Party's redactions.

A Filing Party receiving redacted Records from a Designating Party is not required to defend the appropriateness of redactions made by a Designating Party under this section in order to file them in the form received, after providing the Notice set forth in Model Rule 3.0(C). This provision does not preclude a receiving party from objecting to or challenging redactions by a Designating Party.

❖ *COMMENT*

The Model Rule provides that a Filing Party need not defend a Designating Party's redactions of Presumptively Protected Information as a result of filing the redacted materials as received. Indeed, a Filing Party may object to or challenge those redactions. The justification for making the redactions remains the Designating Party's burden.

(D) Redactions to be no more extensive than required.

Redactions to prevent unauthorized public disclosure of information described in Model Rule 1.0(F) should be no more extensive than required to maintain the confidentiality of the Presumptively Protected

Information, and should not, where feasible, obscure the type of information being redacted, if the nature of the type of information is indicated on the original document: *for example*, "D.O.B.___".

❖ *COMMENT*

Section 2.0(A) of the Model Rule requires that redactions of Presumptively Protected Information be "no greater than required to protect" disclosure. This provision states this obligation in a more specific manner to prevent the application of redactions in an overly broad manner that conceals not only the Presumptively Protected Information, but also conceals the type of information being redacted. This occurs, for example, when a redaction on a form conceals a Social Security Number, but also extends to conceal that what is being redacted *is* a Social Security Number, such as the header of the box containing the Social Security Number. Those applying redactions must be instructed not to conceal anything beyond the Presumptively Protected Information itself.

(E) Redactions to be textual where feasible.

To apprise viewers of the bases for redactions, where the technology used to redact provides for textual redactions (as opposed to blackbox or whitebox redaction), textual redactions that characterize the redactions should be used (e.g., "PHI/PII Redacted" or "Personal Protected Information Redacted").

❖ *COMMENT*

Many document review and software platforms that provide the ability to embed redactions on document

images also have redaction format options that allow "text redactions" as well as traditional blackout or whiteout redactions. The use of text redactions to provide a basis for and give context to redactions on the face of a document is preferred to blackout or whiteout redactions of Presumptively Protected Information. If technology does not permit, or if the filing party is pro se and does not have the capabilities to provide textual redactions, the party may use any reasonable method available to redact the Presumptively Protected Information.

3.0 All Other Sealing

(A) Court approval required.

A Record must not be filed under seal or redacted without a court order, except in connection with a Notice of Proposed Sealed Record, or if the Record contains Presumptively Protected Information governed by Model Rule 2.0. A Record filed under seal in connection with a Notice of Proposed Sealed Record will be temporarily sealed unless and until an order disposing the motion to seal is entered, *e.g.*, the "Conditionally Sealed Period." Thereafter, the Record remains sealed unless determined otherwise by an order of the court. See Model Rules 1.0(A), 3.0(F), and 4.0.

❖ *COMMENT*

This Rule permits a Filing Party to file a Record under seal conditionally while a court ruling on the issue is pending. The Model Rule focuses on the procedure for filing under seal and not the substantive requirements for sealing Records. Nothing in the Rule

shall be interpreted to restrict any rights to intervene under Federal Rule of Civil Procedure 24(a) or (b).

(B) CM/ECF filing requirement.

(1) Unless otherwise ordered by the court, any Record to be filed under seal, Notice of Proposed Sealed Record, or motion to seal must be filed electronically with restricted access using the court's CM/ECF System. Notwithstanding this requirement, a Filing Party who is not represented by an attorney (*i.e.*, is "pro se") must not file electronically unless the pro se is approved to become a CM/ECF user in that case pursuant to local rules or court order. If a pro se party is not an approved CM/ECF user, the pro se must file such documents in paper form, and the Clerk of Court will perform the necessary filing steps in the CM/ECF system.

(2) Proposed Sealed Records are to be filed only with the underlying motion, pleading, or response, and each such Record shall be filed separately so that each document is assigned its own ECF docket number (*e.g.*, ECF No. 2, or ECF No. 2-2). The Proposed Sealed Record(s) must be filed as separate docket entries in both sealed and unsealed and redacted and unredacted forms. Any Filing Party must file a Notice of Proposed Sealed Record pursuant to Model Rule 3.0(C).

(3) Nonpublic Filing of Proposed Sealed or Redacted Records. An unsealed or unredacted copy of each Proposed Sealed or Redacted Record must be filed concurrently with the motion, pleading, or response to which the Proposed Sealed or Redacted

Record(s) are referenced or attached, using CM/ECF restricted viewing. All Records filed under seal or in unredacted form must state "FILED CONDITIONALLY UNDER SEAL" at the top of the Record or in such a place so as not to obscure the content of the document.

(4) Publicly Filed Versions of Proposed Sealed and Redacted Records. Redacted Records must be filed in redacted form in the public record. A Record to be sealed in its entirety must be filed in the public record by a placeholder slip sheet stating "DOCUMENT FILED UNDER SEAL." Each Proposed Sealed Record that is an attachment to a filing must be numbered (*e.g.*, as "Sealed Exhibit Number ___" and "Redacted Exhibit Number ___").

❖ *COMMENT*

These sections of the Model Rule discuss the process for filing Records under seal using the CM/ECF system. The Proposed Sealed and/or Redacted Records are filed ***just one time***, concurrently with the motion, pleading, or response to which the Proposed Sealed or Redacted Record are referenced. The Proposed Sealed or Redacted Record will be referenced by ECF docket number in both the Notice of Proposed Sealed Record and motion to seal, and is not to be attached to the Notice, the motion to seal, or any declaration filed in support. The purpose of this requirement is to prevent repetitious filings, reduce the burden on the courts, and lessen the likelihood of inconsistent sealed or redacted filings. See Model Rule 3.0(C) and (D) and discussion below. The Notice is to be filed after the underlying motion, pleading, or response,

so that the Notice may referenced the Proposed Sealed or Redacted Records by docket number.

The Form Notice that this *Commentary* has devised and proposes be uniformly used for efficiency and consistency contains a dropdown feature to identify whether there are any known objections to the proposed Sealed Records. The functionality of this dropdown feature, unfortunately, is not available when the Form is incorporated within these materials. Available options include: Yes, No, and Unknown.

This *Commentary* understands that some district courts require that documents requested to be filed under seal or redacted be submitted in hard-copy ("paper") form.[7] This *Commentary* elects to require the use of ECF to adopt modern filing requirements and alleviate the burden on courts to manage paper files or external media containing such files. This *Commentary* also considered that requiring another submission in paper form adds an extra layer of complexity and security for the parties and the court, and therefore removed such a requirement from this Model Rule. This *Commentary* acknowledges a court may still want a paper copy of sealed or redacted Records in limited circumstances, or may need to require paper copies in the instance of filers who have not been approved as ECF users in the case, and so included

7. *See*, *for example*, C.D. Cal. L.R. 79-5.2.1(b); *see also*, W.D.N.Y., L.R. 5.3; E.D. Pa. L.R. 5.1.2; W.D. Pa. CM/ECF Manual. Other courts permit a choice of either manual or ECF filing. *See*, *e.g.*, N.D. Cal. L.R. 79-5. While other courts require that such documents be filed only via ECF. *See* E.D. Tex. L.R. CV-5(a)(7)(D); N.D.N.Y. L.R. 5.3(a) (former L.R. 83.13(6)); and D. Del. Electronic Case Filing CM/ECF User Manual XIV.C.

3.0(B)(4)(b) in the Model Rule.[8] As another example, recent CM/ECF data breach issues have caused jurisdictions around the country to issue specific guidance on filing highly sensitive documents in paper form or via other secure means.[9]

The Model Rule also requires the use of placeholder slip sheets in place of the sealed Record to make it easier to track the Record, and to consistently identify it by the same exhibit number from the time the Record is filed with the original motion, pleading, or response that cites to Sealed or Redacted Records, through the filing of the Notice of Proposed Sealed Record by the Filing Party (*see* 3.0(C)), and in the motion to seal and supporting declaration later filed by the Designating Party, which seeks to keep the information protected (*see* 3.0(D)). Placeholder slip sheets are commonly used by other courts.[10]

Grouping Sealed and Redacted Documents Together In One Docket Entry: Current CM/ECF filing capabilities require filers to group all redacted or sealed documents together in a single docket entry. This is because current CM/ECF capabilities do permit e-service of sealed documents (though all courts do not currently use this

8. *See, for example*, N.D.N.Y. L.R. 5.3(a) (former L.R. 83.13) (requiring a motion to seal to be via ECF, but also requiring that "copies of all documents sought to be sealed be provided to the Court, for its in camera consideration, as an attachment in .pdf form to an email to the judge").

9. *See Judiciary Addresses Cybersecurity Breach: Extra Safeguards to Protect Sensitive Court Records* (Jan. 6, 2021), U.S. COURTS, https://www.uscourts.gov/news/2021/01/06/judiciary-addresses-cybersecurity-breach-extra-safeguards-protect-sensitive-court.

10. *See* N.D.N.Y. L.R. 5.3 (former L.R. 83.13(6)).

functionality), but only if the documents are grouped together in a single docket entry. For example, a filing of sealed documents or unredacted versions of documents would look like this:

1	COMPLAINT filed by Plaintiff Allison Apple (Smith, Joe) (Filed on 03/01/2021)(Entered: 03/01/2021)
2	NOTICE of MOTION to dismiss filed by XYC Corporation (Attachments: # 1 MEMORANDUM in Support, # 2 Proof of Service, # 3 Proposed Order) (Jones, Jessica) (Filed on 04/30/2021)(Entered: 04/30/2021)
3	DECLARATION of Jessica Jones in support of 2 MOTION to dismiss filed by XYZ Corporation (Attachments: #1 Redacted Exhibit No. 1; # 2 Sealed Exhibit No. 2; # 3 Redacted Exhibit No. 3; # 4 Sealed Exhibit No. 4, # 5 Exhibit No. 5, # 6 Exhibit No. 6, # 7 Exhibit No. 7)(Jones, Jessica) (Filed on 04/30/2021)(Entered: 04/30/2021)
4	PROPOSED SEALED DOCUMENTS for 3 Declaration of Jessica Jones filed by XYZ Corporation (Attachments: #1 Unredacted Version of Exhibit No. 1; # 2: Sealed Exhibit No. 2; # 3 Unredacted Version of Exhibit No. 3; # 4 Sealed Exhibit No. 4) (Jones, Jessica) (Filed on 04/30/2021)(Entered: 04/30/2021)
5	NOTICE OF PROPOSED SEALED Records filed by XYZ Corporation (Jones, Jessica)(Filed on 04/30/2021) (Entered: 04/30/2021)

In the above example, party XYZ Corporation filed a motion to dismiss (ECF No. 2) and is filing exhibits in support. (ECF Nos. 3, 4). All the documents in ECF No. 3 are filed publicly. ECF Nos. 3-1 and 3-3 are redacted versions of Proposed Redacted Records. ECF Nos. 3-2 and 3-4 are the cover slip sheets for two documents filed under seal. ECF Nos. 3-5, 3-6, and 3-7 are exhibits not subject to any sealing or redacting requests and are simply filed in the public view.

All the documents filed in ECF No. 4 are filed under seal, away from public viewing until the motion to seal can be ruled upon. ECF Nos. 4-2 and 4-4 are unredacted versions of ECF 3-2 and 3-4. ECF Nos. 4-3 and 4-5 are unsealed versions of the entirely sealed ECF Nos. 3-3 and 3-5. The

proper classification of these filings within a court's CM/ECF system will differ by local rules and ECF filing guidelines. A possible option would be to file these under the option "Exhibit."

By grouping these Proposed Sealed and Redacted Records together, filers can use the CM/ECF system to e-serve the unsealed and unredacted versions on relevant parties and registered ECF non-parties, rather than having to separately serve them via a different mechanism. This *Commentary* understands that while not all courts use this ECF functionality to permit e-service of unsealed and unredacted versions of Proposed Sealed or Redacted Records, many districts do.[11] It is the hope that increased ECF functionality will, in the future, not require that all Proposed Sealed and Redacted Records be grouped together in one docket entry.

In the example above, ECF No. 5 is the Notice of Proposed Sealed Record, which is a form that is to be filed immediately after any motion, pleading, or response seeking to file sealed or redacted documents, which is discussed below. See Comment re. Model Rule 3.0(C), below, and Notice of Proposed Sealed Record form, above.

(5) Filing a document under seal does not exempt the filer from the service requirements imposed by federal statutes, rules, or regulations or by a court's local rules. E-service on parties in sealed or

11. *See, for example*, District of Minnesota L.R. 5.6 and its Sealed Civil User's Manual.

unredacted forms will be accomplished through the CM/ECF system, where available. If CM/ECF service is unavailable for such Records, a Filing Party who is an approved CM/ECF user must accomplish service same day as otherwise required by the Federal Rules of Civil Procedure, Federal Rules of Criminal Procedure, and Local Rules. Service on a pro se party or non-party who has not been previously approved to be a CM/ECF user in the case must be made in accordance with Federal Rule of Civil Procedure 5.

❖ *COMMENT*

This *Commentary* acknowledges that not all courts currently use the full functionality of the CM/ECF system. The CM/ECF system does have the functionality to permit parties to view Sealed and Redacted Records in their entirety, as well as to "serve" them via the CM/ECF notification system to registered users, while maintaining those Records as blocked from public view.[12]

(6) The motion to seal and its supporting documents, identified below in Model Rule 3.0(D),

12. *See, for example*, District of Minnesota, Sealed Civil User's Manual (Updated Sept. 28, 2021), https://www.mnd.uscourts.gov/sites/mnd/files/Sealed_Civil_Users_Manual.pdf, at p. 11, providing users with the ability to choose which parties can view unsealed and unredacted version of documents filed out of the public view; *see also* District of Rhode Island, Filing Instructions Civil Motion to Seal, https://www.rid.uscourts.gov/sites/rid/files/documents/cmecf/CivilMotiontoSealFilingInstructions.pdf (same); *see also Judiciary Addresses Cybersecurity Breach: Extra Safeguards to Protect Sensitive Court Records* (Jan. 6, 2021), U.S. COURTS, https://www.uscourts.gov/news/2021/01/06/judiciary-addresses-cybersecurity-breach-extra-safeguards-protect-sensitive-court.

must not be filed under seal or with redactions unless the motion cannot be drafted in a manner that protects the Confidential Information from disclosure.

(7) Any order disposing of a motion to seal should be publicly filed.

❖ *COMMENT*

See discussion on Model Rule 3.0(D), below. While this *Commentary* proposes that the Model Rule be uniformly applied, courts and judges may still have certain individual preferences, which practitioners should be familiar with, including checking standing orders, practical guides, scheduling orders, the judge's webpage, and ECF filing instructions.

(C) Notice of Proposed Sealed Record.

(1) Filing of Notice of Proposed Sealed Record. If a Filing Party intends to file a motion, pleading, or response that references or appends Confidential Information, it must file a Notice of Proposed Sealed Record. A Filing Party must file a Notice of Proposed Sealed Record even if it is the Designating Party.

❖ *COMMENT*

The Notice of Proposed Sealed Record is similar to the District of Maryland's process, requiring the filing of a

Notice of Filing Exhibit or Attachment Under Seal.[13] The purpose of requiring that the Filing Party submit only a Notice of Proposed Sealed Record when filing documents either in redacted form or entirely under seal is to properly place the burden of supporting the sealing of all or part of a Record from the public file on the Designating Party, rather than on the Filing Party. This *Commentary* recognizes that often a party may need to submit documents to a court that another party (or non-party) has designated as Confidential. As a result, that party is required to move to seal the documents, despite not having itself designated the documents as Confidential.

This *Commentary* envisions the Notice itself to be succinct and pro forma and has drafted a fillable Form Notice to accompany the Proposed Model Rule for litigants to use. *See* Notice of Proposed Sealed Record form, above.

(2) Content of Notice of Proposed Sealed Record. The Notice of Proposed Sealed Record must identify each Proposed Sealed or Redacted Record or generally identify the Confidential Information that

13. *See* District of Maryland, Sealed Civil Documents, https://www.mdd.uscourts.gov/content/sealed-civil-documents, https://www.mdd.uscourts.gov/sites/mdd/files/forms/NoticeofFilingofDocumentUnderSeal.pdf. The Northern District of California provides what it calls a "special" procedure for when one party wishes to e-file a document designated confidential by another party, but, in reality, that procedure simply requires that the Filing Party also include information in its declaration in support of the motion to seal identifying that party designated the information as Confidential. *See* Northern District of California, E-Filing Under Seal in Civil Cases, Special Note, https://www.cand.uscourts.gov/cases-e-filing/cm-ecf/e-filing-my-documents/e-filing-under-seal/. This *Commentary* believes this does not adequately place the burden on the Designating Party.

was redacted from each Proposed Sealed or Redacted Record, without disclosing Confidential Information, and identify the corresponding Designating Party. Each Proposed Sealed or Redacted Record shall be referred to the ECF docket number from the motion, pleading, or response to which the Proposed Sealed Records are referenced or attached.

❖ *COMMENT*

The Notice of Proposed Sealed Record contains a section for the Filing Party to identify the reason for redacting or sealing identified records. The *Commentary* envisions that such reason simply may be that the Designating Party designated the records as confidential. Otherwise, if the Filing Party is the Designating Party, a more fulsome description for the proposed reason for sealing may be provided.

(3) Notice Where Records Previously Sealed or Redacted by Court Order. If Records subject to the Notice of Proposed Sealed Record were previously sealed or redacted by court order in the same action, the Filing Party must file a Notice of Proposed Sealed Record in compliance with this section and identify the prior order by ECF docket number and date. A new motion to seal is not required if the court previously ordered the Record sealed or redacted.

(4) Timing of Notice of Proposed Sealed Record. A Notice of Proposed Sealed Record must be filed immediately after any motion, pleading, or response to which the Proposed Sealed or Redacted Records

are referenced or attached (*e.g.*, a motion to compel, a motion for summary judgment, or a motion in limine).

❖ *COMMENT*

Under this section, a Filing Party would file the Notice of Proposed Sealed Record immediately after the pleading, motion, opposition, or response that includes redacted or fully sealed documents. See, for example, Eastern District of Texas Local Rule CV-5(a)(7)(C) and example in Section 3.0(B) above. This *Commentary* proposes that a form be used for greater efficiency and consistency. See Notice of Proposed Sealed Record form. Requiring that the Notice of Proposed Sealed Record be filed immediately after the underlying brief or pleading makes it easy to locate on the docket for both courts and practitioners and allows the Filing Party to identify the Sealed or Redacted Record by ECF number that has been generated. The Notice should be filed as a separate ECF docket entry.

Under many courts' current procedures, the same Sealed or Redacted Record may be filed multiple times in the same action. Model Rule 3.0(C)(3) obviates the need to repeatedly file a motion to seal every time the Sealed or Redacted Record is introduced if the court has already ruled on it being sealed or redacted. In such a circumstance, the Filing Party need only file the Notice of Proposed Sealed Record in compliance with the Model Rule and identify by ECF Docket number and date the prior court decision that orders the sealing or redaction of the Record. The Notice that this *Commentary* proposes allows the Filing Party to indicate whether it is aware of any objection to the filing of the document under seal. See Notice of Proposed Sealed Record form.

The documents proposed to be filed under seal, whether fully sealed or in partially redacted form, are not to be attached to the Notice of Proposed Sealed Record. Both redacted/sealed and unredacted/complete versions of the documents at issue will be filed only once, by the Filing Party with the underlying motion, pleading, or response to which they pertain, in compliance with Model Rule 3.0(B)(3).

Example 1: Filing Party A is filing a motion for summary judgment and seeks to file under seal, as Exhibits 1—6, documents that Filing Party A has previously deemed Confidential. Filing Party A would attach the Exhibits 1—6 in sealed and unsealed form ***only*** to its motion for summary judgment, grouping sealed and redacted documents in one docket entry, and the slip sheets for the sealed documents and redacted versions in the public view grouped in a separate docket entry. See example of and discussion re. Rule 3.0(B) above. The public docket would contain slip sheet placeholders for each Sealed Record. Filing Party A would, immediately after filing its motion for summary judgment, file a Notice of Proposed Sealed Record. The Notice, which is proposed to be a fillable form, identifies Exhibits 1—6 as documents it is conditionally filing under seal by their ECF docket numbers, generally describing the documents in the Notice form: "ECF Nos. ___ are business records Filing Party A produced in this litigation and previously designated Confidential pursuant to the Stipulated Protective Order entered in this case, ECF No. ___".

***Example 2*: Filing Party B is filing an opposition to a motion for summary judgment and must file several of its exhibits, Exhibits 7—12, under seal because they were produced by another party who has designated the

documents Confidential under the Confidentiality Order entered in the case. Filing Party B neither produced nor designated the records Confidential. Filing Party B would attach Exhibits 7—12, in both sealed and unsealed forms grouped together in compliance with Rule 3.0(B)(4) and current CM/ECF capabilities, ***only*** to its opposition, not to its Notice of Proposed Sealed Record. Filing Party B would, immediately after filing its opposition and exhibits in the docket, file a Notice of Proposed Sealed Record form, identifying Exhibits 7—12 as documents it is filing under seal by their ECF docket numbers, generally describing the documents: "ECF Nos. ___ are business records produced by Designating Party X in this litigation that Designating Party X has designated Confidential pursuant to the Stipulated Protective Order entered in this case, ECF No. __."

Example 3: Filing Party C is filing a motion in limine seeking to preclude another party's expert from testifying on certain matters contained within the expert's report. Small portions of the expert's report have been deemed Confidential, as they contain the Designating Party's financial information that it does not wish its competitors to see. While the expert's report is relevant to the motion in limine and therefore must be filed, the confidential financial information can be redacted out, leaving the rest of the report available to public viewing. Filing Party C would file the redacted expert report publicly and the unredacted complete version of the expert's report under seal, as a separate docket entry, ***only*** with its motion in limine, and not with its Notice of Sealed Record. Immediately after filing its motion in limine, Filing Party C would file a Notice of Sealed Records identifying the Confidential Information that Filing Party C redacted out

of the Record by page and line number, for example: "Page 4, lines 10-20 are redacted, as they contain financial information that Designating Party has designated as Confidential."

Example 4: Filing Party D is filing an opposition to a motion to exclude its expert. One of Filing Party D's exhibits is the expert's report, which contains redacted portions that were the subject of a prior motion to seal that was granted by the court earlier in the action. Filing Party D would file the redacted expert report publicly and the unredacted complete version under seal, as a separate docket entry, ***only*** with its opposition to the motion to exclude. Immediately after filing its opposition to the motion to exclude, Filing Party D would file Notice of Proposed Sealed Record identifying on the form the Confidential Information that Filing Party D redacted out by ECF Docket No. and page and line citation, and identify in the Notice the prior court order which approved the redaction of the expert report by date and ECF docket number. The Designating Party would not need to file another motion to seal the report, since the redactions were previously approved by the court.

See also exemplar ECF docket entries in section 3.0(B) above.

(5) Notice to Non-Party Designating Parties. If Records subject to the Notice of Proposed Sealed Record were produced by a Designating Party that is a non-party to the litigation, the Filing Party filing the Notice of Proposed Sealed Record must provide notice of the filing to the non-party in accordance with Rule 3.0(B)(5).

❖ *COMMENT*

This section aims to ensure the filing party gives proper notice to any non-party Designating Parties that Confidential material is being submitted under seal and to give the non-party the opportunity to file a motion to seal and prevent the public dissemination of such Confidential information. Most of the time, this notice to non-parties may be accomplished via email to their counsel, but Rule 3.0(B)(5) also provides mechanisms for service on or by pro se filers or who may be a Designating Party.

(**D**) **Motion to Seal.**

(1) Motion to Seal. If a Designating Party whose Record(s) are the subject of a Notice of Proposed Sealed Record seeks to maintain such Records under Seal, the Designating Party must file a motion to seal. A Filing Party who is the Designating Party must file and serve the motion to seal in compliance with this Rule.

(2) Memorandum. The motion to seal must include a nonconfidential memorandum in support that complies with Model Rule 3.0(B)(6) describing: (a) each Record(s) to be sealed or redacted; (b) the basis for the request; and (c) how each Record(s) to be sealed or redacted meets applicable standards for sealing.

(3) Declaration in Support. The motion to seal must include a nonconfidential declaration in support setting forth the legal basis for filing each Record under seal or in redacted form, and such Records should not be refiled, but should be

identified by their ECF docket numbers from the motion, pleading, or response to which the Proposed Sealed Record(s) is referenced or attached (*e.g.*, ECF No. 2 or ECF No. 2-2).

❖ ***COMMENT***

This procedure places the burden of supporting a request to seal or redact information on the party who produced the document and who therefore has an interest in, and basis for, protecting it from public disclosure. This *Commentary* finds that most of the current sealing rules place the burden to defend redactions and Confidentiality designations on the party that seeks to file the documents under seal, without considering that the Filing Party may not be the Designating Party and may therefore have no interest in sealing the Records (or may be averse to their sealing). This *Commentary* anticipates that shifting the burden of sealing the documents to the Designating Party will reduce overdesignation of information and documents as Confidential.

This *Commentary* also finds it important to limit the number of submissions under seal to the court. After considering various local rules, this *Commentary* proposes that the motion to seal and supporting memorandum and declaration should, wherever possible, be filed in the public view and not under seal. This *Commentary* contends that Designating Parties can adequately describe the document and the nature of the Confidential Information contained in it without the need to provide Confidential Information in the motion

to seal itself.[14] While some courts require that a declaration in support of a motion to seal also be sealed, this proposed Model Rule seeks to limit the number of documents that are sealed from public view and requires that the declaration not be sealed or redacted.

While the Model Rule does not have a meet-and-confer requirement, local rules, standing orders, and stipulated protective orders entered into between the parties may require parties to meet and confer before the filing of any motion, and conferring is always a best practice.[15] Even if the court handling a given case does not have such a requirement, it may help to include in the motion to seal whether the motion is unopposed/uncontested.

When designating documents and information as Confidential, all parties should avoid overdesignation, as moving to seal likely increases case costs over time.[16] This also applies to deposition and hearing transcripts as well as to motions and pleadings. Parties should review transcripts to designate only necessary portions of testimony as Confidential, if possible, rather than designating an entire transcript as Confidential. Parties also should do their best to frame motions, declarations,

14. *See, for example,* W.D. Tex. L.R. 5.2(b) (motions and pleadings under seal are "disfavored"), and (c) (while motions to seal are first filed under seal "the court expects parties to draft sealing motions to seal in a manner that does not disclose confidential information" because "the sealing motion may subsequently be unsealed by court order.").

15. *See, for example*, D.N.J. L.R. 5.3(c)(2) ("Not later than 21 days after the first filing of sealed materials, the parties shall confer in an effort to narrow or eliminate the materials or information that may be the subject of a motion to seal.").

16. *See, for example*, N.D. Cal. L.R. 79-5(b), requiring that all requests to seal "be narrowly tailored."

and pleadings to avoid the quotation or recitation of sealable or Confidential Information, which lessens the likelihood that the underlying motion must be sealed.

(4) Timing of Motion to Seal. A Designating Party must file its motion to seal and supporting declaration within the time frame set for the filing of any responsive pleading to the motion that references or appends a Designating Party's Confidential Information, unless otherwise ordered by the court. If a responsive pleading is not permitted, the motion to seal and supporting declaration must be filed within seven (7) court days of service of the Notice of Proposed Sealed Record.

(5) Failure to Timely Move to Seal. If the Designating Party does not timely file its motion to seal in accordance with this Rule, the Designating Party waives its right to maintain that the Records contain Confidential Information.

❖ *COMMENT*

Recognizing that a Designating Party once in receipt of a Notice of Proposed Sealed Record must act quickly to defend its Confidential information and designations, this *Commentary* considered the number of days that the Designating Party should have to file a Motion to Seal, and considered including up to 14 days and as little as

three days for such filing.[17] Ultimately, this *Commentary* opts to use the deadline of the response brief for the underlying filing as the target date, because such date is tied directly to the underlying filing and will ensure that sealing progresses promptly, avoids confusion and the possibility that a hearing on a motion to seal will be scheduled after the hearing on the underlying motion (if applicable), and avoids multiple deadlines related to the same motion (if applicable) for courts.

If the motion to seal is not timely filed by the Designating Party, the Filing Party must timely file the Confidential Information in unredacted or unsealed form pursuant to this Model Rule. See Model Rule 3.0(F)(1).

(E) Proposed Order. A proposed order must be filed and served with the motion to seal.

❖ ***COMMENT***

The Model Rule requires that a proposed order must be served with every motion to seal, as is currently required in most courts.[18] This *Commentary* has not proposed the substance or basis for the order, as district courts have widely differing standards on the substantive

17. *See, for example*, Northern District of California, E-Filing Under Seal in Civil Cases, Special Note, https://www.cand.uscourts.gov/cases-e-filing/cm-ecf/e-filing-my-documents/e-filing-under-seal/, which requires the designating party to submit a declaration "establishing that all of the designated material is sealable" within four days of the filing of the moving party's administrative motion to seal.

18. *See* N.D.N.Y. L.R. 5.3(a) (former L.R. 83.13(6)) (requiring proposed order).

requirements that must be met for a court to justify removing a document, or a portion of a document, from public view.[19] See Appendix: Standards for Sealing Records.

In many instances, the number of documents to be sealed and redacted are numerous, and many cases involve multiple motions to seal. Parties should consider submitting a proposed order that, in addition to complying with local rules and standing orders, clearly sets forth what is sealed or redacted for future reference and citation.

(F) Disposition of Proposed Sealed Records.

(1) If the Designating Party fails to timely file a motion to seal after receiving Notice pursuant to Model Rule 3.0(C) above, the Filing Party must publicly file the Confidential Information in unredacted and unsealed form within seven (7) court days of the expired motion to seal deadline.

(2) If the court grants the motion to seal, the Proposed Sealed Record will be deemed filed as of the date of the filing of the Notice of Proposed Sealed Record unless otherwise directed by the court.

(3) If the court denies the motion to seal, the Filing Party shall publicly file the Confidential Information

19. Having been tasked with proposing a purely procedural rule, this *Commentary* does not propose the substantive findings a court must make before permitting sealing or redacting a record from public view, if at all. *See, for example*, Kondash v. Kia Motors Am., Inc., 767 F. App'x 635, 637 (6th Cir. 2019) (citation omitted) (setting forth substantive standard that must be met for documents to be filed under seal, on a document-by-document basis).

in unredacted and unsealed form within seven (7) court days of the order denying the motion to seal, or take other action as ordered by the court.

❖ *COMMENT*

This provision derives from similar requirements employed by some federal courts.[20] Such courts require records to be resubmitted after a motion to seal is granted.[21] Further, this provision is intended to lessen the burden on the parties and the clerk as to the resubmission of records under seal pursuant to court order. If an order has been entered sealing Records, resubmission should not be required. But if the order modifies the portions of the records to be sealed, then the applicable order must specify resubmission as to affected records.[22]

4.0 Disposition of Sealed and Redacted Records at the Conclusion of the Case.

Unless otherwise ordered by the Court, a Sealed or Redacted Record will remain sealed or redacted after final disposition of the case. Anyone seeking to unseal or unredact a Record may petition the court by motion. The motion must be served on all parties in the case and upon any Designating Party that is a non-party in accordance with the service requirements in this Rule.

20. *See* N.D. Tex. L.R. 79.3(b)(2) and E.D. Tex. L.R. 5(a)(7)(C).

21. *See, for example,* E.D.N.Y. "Steps for E-filing Sealed Documents – *Civil Case*", at ¶ 2.

22. *See also* W.D. Tex. L.R. CV-5.2(d).

❖ *COMMENT*

Courts differ widely on the disposition of sealed records at the conclusion of a case. Many local rules are silent.[23] Some courts have rules that automatically unseal records after a certain time period.[24] It is always a best practice to check Local Rules.

While this *Commentary* understands that courts may have an interest in unsealing Records on their dockets, the alternatives explored were considered burdensome and could present several unique problems. For example, this *Commentary* considered options like the California Northern District rules, which require automatic unsealing of records after a certain time period unless a motion was filed to extend the sealing. However, since one of the goals of the proposed Model Rule is to lessen the burden on the courts and parties, the automatic unsealing of records was not included because it may not satisfy this goal. Such a rule might generate more court filings by parties seeking to keep records permanently under seal, and courts would have to track the established sealed period. Upon expiration of the sealed period, a court might need to manually unseal each individual document, because the electronic case filing system does not have an automated process to unseal documents. This proposed Rule also expressly

23. The Model Rule in this section is similar to Local Rule 5.3 found in the Western District of New York; *see also* S.D. Miss. L.R. 79(f) and N.D. Miss. L.R. 79(f).

24. For example, the Northern District of California automatically unseals records after 10 years unless ordered otherwise upon a showing of good cause. *See* N.D. Cal. L.R. 79-5(g).

acknowledges that a member of the public or non-party may move to unseal or unredact a document at any time.

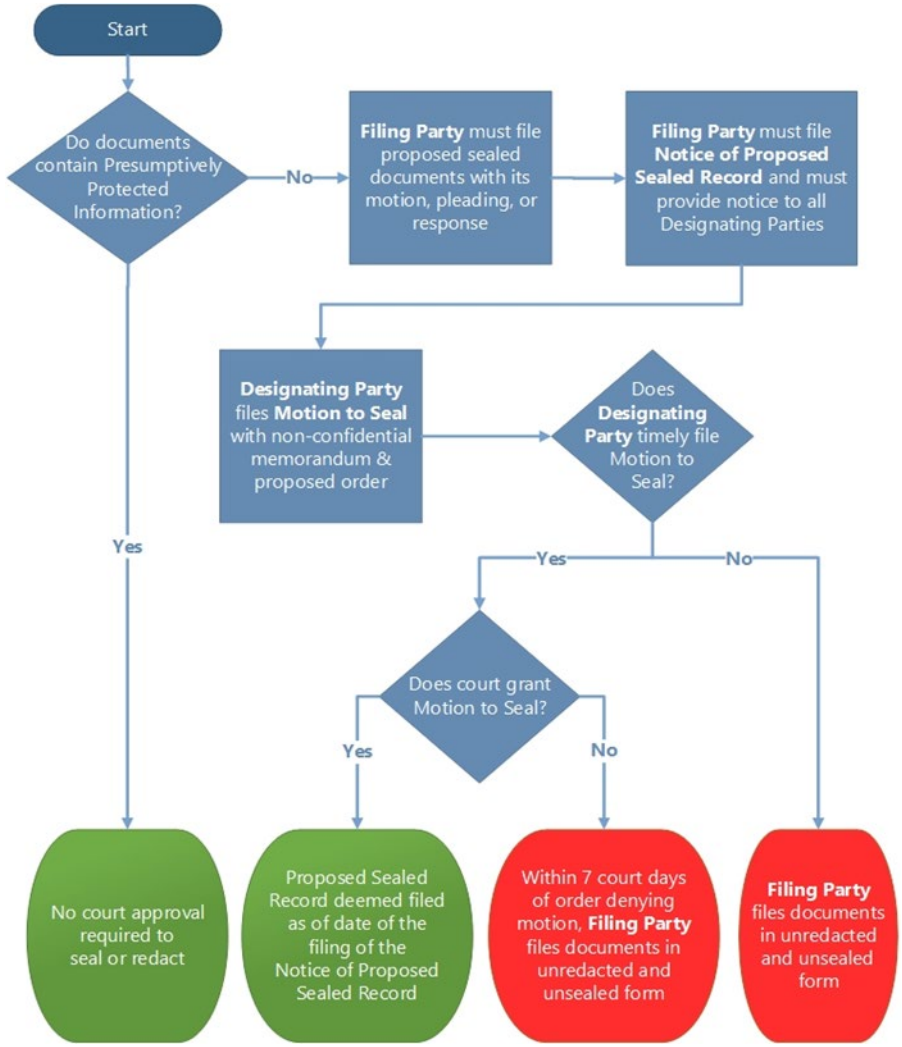
This *Commentary* also considered applying a specified time period for sealing. A shorter time period (such as six months, one year, or two years) may lead to many motions, especially for larger litigation that can continue for several years. A longer time period for the automatic unsealing of records (such as 10 years) poses other problems and burdens. For example, after 10 years, a party that has a serious need to keep records sealed may not be able to locate and provide notice to all interested parties and non-parties. In either scenario, the court would also be burdened with tracking the expiration of the sealing order.

Other courts require a party to state the period of time the party seeks to have records maintained under seal.[25] This *Commentary* rejects the use of such process because it does not lessen the burden on courts to track such a deadline and take action to unseal records.

The Model Rule was designed to protect records that should remain sealed, while providing public access to records should there be an interest in the records. The proposed Model Rule protects the interests of all parties and non-parties while significantly lessening the burden on the courts.

25. *See* E.D. La. L.R. 5.6(B)(4) and E.D. Va. L.R. 5(C)(4).

Model Rule for the Sealing and Redacting of Information Flowchart



IV. APPENDIX: STANDARDS FOR SEALING IN FEDERAL COURTS

Presumptive Right of Access to Judicial Records

"[T]he courts of this country recognize a general right to inspect and copy public records and documents, including judicial records and documents."[26] The right to access is based on the public's "desire to keep a watchful eye on the workings of public agencies."[27] This right derives from common law, the

26. Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 597 (1978).

27. *Id.*, 435 U.S. at 598. *See also In re* Providence Journal Co., 293 F.3d 1, 9 (1st Cir. 2002) (quotation omitted) ("Courts have long recognized 'that public monitoring of the judicial system fosters the important values of quality, honesty and respect for our legal system.'"); United States v. Amodeo (*Amodeo II*), 71 F.3d 1044, 1048 (2d Cir. 1995) (quotation omitted) ("The presumption of access is based on the need for federal courts, although independent—indeed, particularly because they are independent—to have a measure of accountability and for the public to have confidence in the administration of justice."); Littlejohn v. BIC Corp., 851 F.2d 673, 678 (3d Cir. 1988) ("As with other branches of government, the bright light cast upon the judicial process by public observation diminishes possibilities for injustice, incompetence, perjury, and fraud."); Columbus-Am. Discovery Grp. v. Atlantic Mut. Ins. Co., 203 F.3d 291, 303 (4th Cir. 2000) ("Publicity of such records, of course, is necessary in the long run so that the public can judge the product of the courts in a given case. It is hardly possible to come to a reasonable conclusion on that score without knowing the facts of the case."); SEC v. Van Waeyenberghe, 990 F.2d 845, 849 (5th Cir. 1993) (citation omitted) ("Public access [to judicial records] serves to promote trustworthiness of the judicial process, to curb judicial abuses, and to provide the public with a more complete understanding of the judicial system, including a better perception of its fairness."); Citizens First Nat. Bank of Princeton v. Cincinnati Ins. Co., 178 F.3d 943, 945 (7th Cir. 1999) ("the public at large pays for the courts and therefore has an interest in what goes on at all stages of a judicial proceeding."); IDT Corp. v. eBay, 709 F.3d 1220, 1222 (8th Cir. 2013) (citing *Nixon*, 435 U.S. at 597) ("This right of access bolsters public confidence in the judicial system by allowing citizens to evaluate the reasonableness and fairness of judicial proceedings

First Amendment, or both. Distinct from these rights is Rule 26(c) of the Federal Rules of Civil Procedure, which permits courts to protect documents and information exchanged during discovery. As detailed below, courts differ in their application of the common law and First Amendment and their definition of whether a particular document to be sealed is indeed a "judicial record." The procedures to be followed for sealing documents also differ.[28]

A. Common Law Right of Access

The common law public right of access, unlike a Rule 26(c)[29] inquiry by comparison, begins with a presumption in favor of public access.[30] The common law right of access "antedates the Constitution" and it attaches to both judicial proceedings and records, in both criminal and civil cases.[31] This common law

---

and 'to keep a watchful eye on the workings of public agencies.'"); Ctr. for Auto Safety v. Chrysler Grp., LLC, 809 F.3d 1092, 1096 (9th Cir. 2016), *cert. denied*, 137 S.Ct. 38 (Oct. 3, 2016) (quoting *Amodeo II*, 71 F.3d at 1048) ("The presumption of access is 'based on the need for federal courts, although independent—indeed, particularly because they are independent—to have a measure of accountability and for the public to have confidence in the administration of justice.'"); United States v. Hickey, 767 F.2d 705, 708 (10th Cir. 1985) ("The right is an important aspect of the overriding concern with preserving the integrity of the law enforcement and judicial processes."); Romero v. Drummond Co., 480 F.3d 1234, 1245 (11th Cir. 2007) (citation and internal citation omitted) ("the common-law right of access to judicial proceedings, an essential component of our system of justice, is instrumental in securing the integrity of the process.").

28. The drafters of this *Commentary* reviewed Appellate Rules, Local District Court Rules, and ECF rules and found little uniformity on procedures for sealing.

29. Hereinafter, all references to "the Rule" or "Rules" shall refer to the Federal Rules of Civil Procedure unless expressly stated otherwise.

30. *In re* Avandia Mktg., Sales Practices and Prods. Liab. Litig., 924 F.3d 662, 670 (3d Cir. 2019).

31. *Id.*, at 672.

right, however, is not absolute, but is left to the "sound discretion of the trial court, a discretion to be exercised in light of the relevant facts and circumstances of the particular case."[32] Because every court has inherent, supervisory power over its own records and files, even where a right of public access exists, a court may deny access where it determines that the court-filed documents may be used for improper purposes. Examples include the use of records "to gratify private spite or promote public scandal" or to circulate libelous statements or release trade secrets.[33]

B. First Amendment Right of Access

The Supreme Court has held that the First Amendment guarantees the public and the press the right of access to criminal trials.[34] Although the Supreme Court has not specifically extended the First Amendment right of public access to civil proceedings,[35] many courts have done so.[36] The constitutional right

32. *Nixon*, 435 U.S. at 598–99.

33. *Id*.

34. Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 580 (1980).

35. *Id*. at n.17 ("Whether the public has a right to attend trials of civil cases is a question not raised by this case, but we note that historically both civil and criminal trials have been presumptively open.").

36. *See, e.g.*, Publicker Indus., Inc. v. Cohen, 733 F.2d 1059, 1070 (3d Cir. 1984) ("A presumption of openness inheres in civil as well as criminal trials."). *See also* Westmoreland v. Columbia Broad. Sys., Inc., 752 F.2d 16, 23 (2d Cir. 1984) (asserting that "the First Amendment does secure to the public and to the press a right of access to civil proceedings"); Rushford v. New Yorker Magazine, Inc., 846 F.2d 249, 253 (4th Cir. 1988) (holding that the "rigorous First Amendment standard should also apply to documents filed in connection with a summary judgment motion in a civil case"); Brown & Williamson Tobacco Corp. v. F.T.C., 710 F.2d 1165, 1178 (6th Cir. 1983) (" The Supreme Court's analysis of the justifications for access to the criminal courtroom apply as well to the civil trial."); *In re* Cont'l Ill. Sec. Litig., 732 F.2d

of access, however, has been found to have a more limited scope in civil context than it does in the criminal.[37] In limiting the public's access to civil trials where the First Amendment applies, there must be a showing that the denial serves an important governmental interest and that there is no less restrictive way to serve that governmental interest.[38] A party seeking the removal of a document from the public eye bears the burden of establishing that there is good cause that disclosure will work a clearly defined and serious injury to the party seeking closure, and the injury must be shown with specificity.[39]

C. Federal Rule 26(c)

Federal Rule of Civil Procedure 26(c) permits a court upon a motion of a party to enter into a protective order to shield a party from "annoyance, embarrassment, undue oppression, or undue burden or expense."[40] Rule 26(c)'s procedures "replace[] the need to litigate the claim to protection document by document," and instead "postpones the necessary showing of 'good cause' required for entry of a protective order until the

1302, 1308 (7th Cir. 1984) ("we agree with the Sixth Circuit that the policy reasons for granting public access to criminal proceedings apply to civil cases as well.").

37. Chicago Tribune Co. v. Bridgestone/Firestone, Inc., 263 F.3d 1304, 1310 (11th Cir. 2001) (citing Newman v. Graddick, 696 F.2d 796, 800–01 (11th Cir. 1983)).

38. *Publicker*, 733 F.2d at 1070 (citing Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 606–07 (1982); *Brown & Williamson Tobacco Corp.*, 710 F.2d at 1179).

39. *Publicker*, 733 F.2d at 1071; *see also In re* Avandia Mktg., Sales Practices and Prods. Liab. Litig., 924 F.3d 662, 673 (3d Cir. 2019), quoting *Publicker*.

40. FED. R. CIV. P. 26(c)(1).

confidential designation is challenged."[41] The trial court has complete discretion over the entry of document protective orders. [42]

A protective order is "intended to offer litigants a measure of privacy, while balancing against this privacy interest the public's right to obtain information concerning judicial proceedings." Rule 26(c) requires that "a party wishing to obtain an order of protection over discovery material must demonstrate that 'good cause' exists for the order of protection."[43] "Good cause" is established on a showing that disclosure will work a clearly defined and serious injury to the party seeking closure; the injury must be shown with specificity.[44] The burden of justifying the confidentiality of each document sought to be covered by a protective order remains on the party seeking the order.[45] Federal courts have superimposed a balancing of interests approach for Rule 26's good cause requirement, requiring courts to balance the party's interest in obtaining access against the other party's interest in keeping the information confidential.[46]

While a protective order entered under Rule 26 generally governs the exchange of confidential information during discovery, it does not typically protect confidential information

41. *Chicago Tribune*, 263 F.3d at 1307–08 (citing *In re* Alexander Grant & Co. Litig., 820 F.2d 352, 356 (11th Cir. 1987)).

42. Seattle Times v. Rhinehart, 467 U.S. 20, 36 (1984) (Rule 26(c) "confers broad discretion on the trial court to decide when a protective order is appropriate and what degree of protection is required.").

43. Pansy v. Borough of Stroudsburg, 23 F.3d 772, 786 (3d Cir. 1994), quoting FED. R. CIV. P. 26(c).

44. *Publicker*, 733 F.2d at 1070.

45. Cipollone v. Liggett Grp., Inc., 785 F.2d 1108, 1121 (3d Cir. 1986), *cert. denied*, 484 U.S. 976 (1987).

46. *Chicago Tribune*, 263 F.3d at 1313 (citing Farnsworth v. Procter & Gamble Co., 758 F.2d 1545, 1547 (11th Cir. 1985)).

from ultimately being filed in the public record, as that is a determination for a court to make, often on a document-by-document basis.[47]

D. Overview of Circuit Case Law

1. First Circuit

In the First Circuit there are "two related but distinct presumptions of public access to judicial proceedings and records" under both the common law right and the First and Fourteenth Amendments.[48]

Under the common law analysis,[49] "judicial records" are those "materials on which a court relies in determining the litigants' substantive rights."[50] "[R]elevant documents which are submitted to, and accepted by, a court of competent jurisdiction in the course of adjudicatory proceedings, become documents to which the presumption of public access applies."[51] Such materials are distinguished from those that "relate[ ] merely to the

47. *See* Shane Grp., Inc. v. Blue Cross Blue Shield of Mich., 825 F.3d 299, 305 (6th Cir. 2016) ("[T]here is a stark difference between so-called 'protective orders' entered pursuant to the discovery provisions of Federal Rule of Civil Procedure 26, on the one hand, and orders to seal court records, on the other . . . Secrecy is fine at the discovery stage, before the material enters the judicial record . . . At the adjudication stage, however, very different considerations apply.").

48. United States v. Kravetz, 706 F.3d 47, 52 (1st Cir. 2013).

49. "While the two rights of access [common law versus First Amendment] are not coterminous, courts have employed much the same type of screening in evaluating their applicability to particular norms." *In re* Providence Journal, 293 F.3d 1, 10 (1st Cir. 2002) (internal citation omitted).

50. *Id.* at 9–10, quoting Anderson v. Cryovac, Inc., 805 F.2d 1, 13 (1st Cir. 1986).

51. F.T.C. v. Standard Fin. Mgmt. Corp., 830 F.2d 404, 409 (1st Cir. 1987).

judge's role in management of the trial."[52] Materials filed with the court relating only "'to the judge's role in management of the trial' and which 'play no role in the adjudication process'" are excluded from the common law presumption of access.[53] For example, the First Circuit classifies civil discovery motions and the materials filed with them as falling within this category, holding that the common law right to public access does not apply to such materials.[54] The First Circuit applies the Rule 26(c) "good cause" standard when deciding whether to protect such documents from disclosure.[55] "A finding of good cause must be based on a particular factual demonstration of potential harm, not on conclusory statements."[56]

For documents that do play a role in the adjudication process and to which the presumption of access therefore applies, common law applies the "compelling need" standard: "only the most compelling reasons can justify non-disclosure of judicial records that come within the common-law right of access."[57]

---

52. *In re* Boston Herald, Inc., 321 F.3d 174, 189 (1st Cir. 2003) (quoting *Standard Fin. Mgmt. Corp.*, 830 F.2d at 408).

53. *Kravetz*, 706 F.3d at 54 (quoting *In re Boston Herald, Inc.*, 321 F.3d at 189; *Standard Fin. Mgmt. Corp.*, 830 F.2d at 408).

54. *Kravetz*, 706 F.3d at 56 (citing *Anderson*, 805 F.2d at 11–13).

55. *Anderson*, 805 F.2d at 7.

56. *Id.* at 19.

57. *Standard Fin. Mgmt. Corp.*, 830 F.2d at 410 (quoting *In re* Knoxville News-Sentinel Co., 723 F.2d 470, 476 (6th Cir. 1983)); *see also, e.g.*, Panse v. Shah, 201 F. App'x. 3, 3 (1st Cir. 2006) ("Sealing is disfavored as contrary to the presumption of public access to judicial records of civil proceedings. It is justified only for compelling reasons and with careful balancing of competing interests.") (citations omitted).

The First Circuit considers the privacy rights of parties to be a compelling reason justifying the sealing of a document from the public eye.[58]

In determining if the First Amendment right of access applies, the First Circuit applies the Supreme Court's *Press-Enterprise II* "experience and logic" test, which asks (1) whether the document is one that has historically been accessible to the press and the public; and (2) whether public access plays a significant positive role in the functioning of the particular process the record concerns.[59] Upon undertaking this analysis, but before sealing a judicial document, the First Circuit mandates that the court issue "particularized findings"[60] and that where some portions of a document may be sealed, "redaction remains a viable tool for separating this information from that which is necessary to the public's appreciation of [the court's order]."[61]

2. Second Circuit

The Second Circuit recognizes both the common law right of access as well a qualified First Amendment right.[62] Like the First Circuit, not all court documents are considered "judicial documents," and "the mere filing of a paper or document with the

58. *Standard Fin. Mgmt. Corp*., 830 F.2d at 411 ("[P]rivacy rights of participants and third parties are among those interests which, in appropriate cases, can limit the presumptive right of access to judicial records."); *Kravetz*, 706 F.3d at 63 (quoting *In re Boston Herald*, 321 F.3d at 190 (Medical information is, as intimated above, "universally presumed to be private, not public.")).

59. *Kravetz*, 706 F.3d at 53–54 (quoting Press-Enterprise Co. v. Superior Court of Calif. for Riverside Cty. (*Press-Enterprise II*), 478 U.S. 1, (1986)).

60. *Kravetz*, 706 F.3d at 61.

61. *Id*. at 63.

62. Hartford Courant Co. v. Pellegrino, 380 F.3d 83, 91 (2d Cir. 2004).

court is insufficient to render that paper a judicial document subject to the right of public access[]" under the common law.[63]

A "judicial document" or "judicial record" (a term used interchangeably) is a filed item that is "relevant to the performance of the judicial function and useful in the judicial process."[64] The presumption of the right of access is "at its zenith" where documents "directly affect an adjudication, or are used to determine litigants' substantive legal rights," and is at its weakest where a document is neither used by the court nor "presented to the court to invoke its powers or affect its decisions."[65] However, a document is "judicial" not only if the judge actually relied on it, but also if the "judge *should* have considered or relied upon [it] but did not."[66] Such documents "are just as deserving of disclosure as those that actually entered into the judge's decision."[67] Documents submitted to the court exist on a "continuum," spanning those that play a role in "determining litigants' substantive rights," which are afforded "strong weight," to those that play only a "negligible role in performance of Article III duties . . . such as those passed between the parties in discovery," which lie "beyond the presumption's reach."[68]

---

63. United States v. Amodeo, 44 F.3d 141, 145 (2d Cir. 1995); U.S. CONST. amend. I; Trump v. Deutsche Bank AG, 940 F.3d 146 (2d Cir. 2019) (rejecting the Third Circuit's determination that any document physically on file with a court is a "judicial record" and aligning more with the First Circuit).

64. Lugosch v. Pyramid Co. of Onondaga, 435 F.3d 110, 119 (2d Cir. 2006).

65. Bernstein v. Bernstein Litowitz Berger & Grossmann LLP, 814 F.3d 132, 142 (2d Cir. 2016).

66. *Id.* at 140, n.3, quoting *Lugosch*.

67. *Id*.

68. United States v. Amodeo (*Amodeo II*), 71 F.3d 1044, 1049–50 (2d Cir. 1995).

The most common judicial records are those submitted in connection with a request for summary adjudication. "[D]ocuments submitted to a court for its consideration on a summary judgment motion are—as a matter of law—judicial documents to which a strong presumption of access attaches . . . ."[69] Documents submitted in support of a motion to dismiss likewise are subject to a presumption of access since they relate to a merits-based adjudication.[70] In contrast, there is no presumption of access to "documents that play no role in the performance of Article III functions, such as those passed between the parties in discovery."[71]

Once the court determines that the document is in fact a judicial document and the strength of the presumption that attaches to that document, the "court must 'balance competing considerations against it,'" such as "'the danger of impairing law enforcement or judicial efficiency' and 'the privacy interests of those resisting disclosure.'"[72] Motions to seal documents must be "carefully and skeptically review[ed] . . . to insure that there really is an extraordinary circumstance or compelling need" to seal the documents from public inspection.[73]

Under the First Amendment, the Second Circuit applies the Supreme Court's *Press-Enterprise II* "experience and logic" test.[74] Once the court finds that a qualified First Amendment right of access to certain judicial documents exists, documents may still

69. Brown v. Maxwell, 929 F.3d 41, 47 (2d Cir. 2019).

70. Shetty v. SG Blocks, Inc., No. 20-cv-00550-ARR-SMG, 2020 WL 3183779, at *10 (E.D.N.Y. June 15, 2020) (citing *Lugosch*, 435 F.3d at 121).

71. S.E.C. v. TheStreet.com, 273 F.3d 222, 232 (2d Cir. 2001); *see also Brown*, 929 F.3d at 50.

72. *Lugosch*, 435 F.3d at 120 (quoting *Amodeo II*, 71 F.3d at 1050).

73. Video Software Dealers Ass'n v. Orion Pictures Corp., 21 F.3d 24, 27 (2d Cir. 1994).

74. *Lugosch*, 435 F.3d at 120.

be sealed, but only if "specific, on the record findings are made demonstrating that closure is essential to preserve higher values and is narrowly tailored to serve that interest."[75] As an example of the application of this test, the Second Circuit has held that attorney-client privilege can be a compelling reason to defeat the presumption of a right of access to judicial documents submitted in opposition to motions.[76] The Second Circuit urges district courts to expeditiously determine whether a document submitted to the court is a judicial document, to avoid impairing the First Amendment rights of a party or the public.[77]

3. Third Circuit

The Third Circuit recognizes a common law and First Amendment right of access.[78] Under a common law inquiry, whether the right of access applies to a particular document or record "turns on whether that item is considered to be a 'judicial record.'"[79] A "judicial record" is a document that "has been filed with the court . . . or otherwise somehow incorporated or integrated into a district court's adjudicatory proceedings."[80] Once a

75. *In re* N.Y. Times Co., 828 F.2d 110, 116 (2d Cir. 1987).

76. *Lugosch*, 435 F.3d at 125.

77. *Id.* at 127. "[T]he loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury." Paulsen v. County of Nassau, 925 F.2d 65, 68 (2d Cir. 1991) (quoting Elrod v. Burns, 427 U.S. 347, 373 (1976)). *Lugosch*, 435 F.3d at 127.

78. *In re* Avandia Mktg., Sales Practices & Prods. Liab. Litig., 924 F.3d 662, 669 (3d Cir. 2019).

79. *Id.*, 924 F.3d at 672 (quoting *In re* Cendant Corp., 260 F.3d. 183 at 192 (3d Cir. 2001).

80. *In re Avandia Mktg.*, 924 F.3d at 672. While filing clearly establishes a document as a judicial record in the Third Circuit, absent a filing a document may still be construed as a judicial record if a court interprets or enforces the terms of the document. *In re Cendant*, 260 F.3d at 192.

document becomes a judicial record, a presumption of access attaches.[81]

The Third Circuit does not distinguish between material filed in connection with a motion for summary judgment and material filed for any other purpose.[82]

At common law, a party wishing to rebut the strong presumption of public access has the burden "to show that the interest in secrecy outweighs the presumption."[83] The movant must show "that the material is the kind of information that courts will protect and that disclosure will work a clearly defined and serious injury to the party seeking closure."[84] The court in its determination must articulate compelling and countervailing interests to be protected, make specific findings on the record about the effects of disclosure, and provide an opportunity for third parties to be heard.[85] The court should conduct a "document-by-document review" of the contents of the materials sought to be sealed.[86] "[B]road allegations of harm, bereft of specific examples or articulated reasoning, are insufficient" to overcome the strong presumption of public access.[87]

---

81. *See id.* at 192–93.

82. *In re Avandia*, 924 F.3d at 672–73; *see also* Leucadia, Inc. v. Applied Extrusion Tech., Inc., 998 F.2d 157, 164 (3d Cir. 1993) ("We see no reason to distinguish between material submitted in connection with a motion for summary judgment and material submitted in connection with a motion for preliminary injunction . . . .").

83. Bank of Am. Nat. Trust & Sav. Ass'n v. Hotel Rittenhouse Assocs., 800 F.2d 339, 343 (3d Cir. 1986).

84. *In re Avandia*, 924 F.3d at 672 (quoting Miller v. Indiana Hosp., 16 F.3d 549, 551 (3d. Cir. 1994)).

85. *In re Avandia*, 924 F.3d at 672–73 (citing *In re Cendant Corp.*, 260 F.3d at 194).

86. *In re Avandia*, 924 F.3d at 673.

87. *In re Cendant Corp.*, 260 F.3d at 194.

While the Third Circuit has recognized that the right of public access enjoyed under the First Amendment as historically applied to criminal trials also applies to civil proceedings,[88] it also acknowledges that, still, "[t]he First Amendment right of access requires a much higher showing than the common law right [of] access before a judicial proceeding can be sealed."[89] In this respect, the Third Circuit follows the "experience and logic" test, just as in the First and Second Circuits.[90]

4. Fourth Circuit

In the Fourth Circuit, the right of public access to judicial documents "derives from two independent sources: the First Amendment and the common law," and accordingly, the Fourth Circuit applies two tests when considering whether any specific document may be filed under seal (or unsealed).[91] Because the common law and First Amendment invoke different standards for assessing the right of access, the district court must identify which is the source of the right of access before balancing the claimed interests.[92]

Under the common law test, when a party asks to seal judicial records, trial courts within the Fourth Circuit "must determine the source of the right of access with respect to each document," and then "weigh the competing interests at stake."[93] The

88. *See* Publicker Indus., Inc. v. Cohen, 733 F.2d 1059, 1070 (3d Cir. 1984).

89. *In re Cendant Corp.*, 260 F.3d at 198 n.13.

90. *In re Avandia*, 924 F.3d at 673.

91. *In re* United States for an Order Pursuant to 18 U.S.C. Section 2703(D), 707 F.3d 283, 290 (4th Cir. 2013).

92. Va. Dep't of State Police v. Washington Post, 386 F.3d 567, 576 (4th Cir. 2004); Co. Doe v. Pub. Citizen, 749 F.3d 246, 266 (4th Cir. 2014); Under Seal v. Under Seal, 230 F.3d 1354 (4th Cir. 2000) (remanding in part because district court failed to identify source of public's right of access).

93. *Va. State Police*, 386 F.3d at 576.

court must also (1) give the public notice and a reasonable opportunity to challenge the request to seal; (2) "consider less drastic alternatives to sealing"; and (3) if it decides to seal, make specific findings and state the reasons for its decision to seal over the alternatives.[94] Under the First Amendment test, like the First, Second, and Third Circuits discussed above, the Fourth Circuit similarly follows the "experience and logic" test.[95]

"Judicial records" in the Fourth Circuit are documents filed with the court that "play a role in the adjudicative process, or adjudicate substantive rights."[96] As examples, motions for summary judgment and the documents attached to those motions are judicial records, even if the attached documents were discovery documents previously covered by a protective order.

Unlike the other Circuits, the Fourth Circuit has not explicitly resolved whether discovery motions and materials attached to discovery motions are judicial records.[97] Some district courts, however, have predicted that the Fourth Circuit will find no public right of access to discovery motions and related exhibits, and that consequently, such documents may be sealed.[98]

5. Fifth Circuit

The Fifth Circuit has held that along with the First Amendment right, there is a right of public access derived from common law that creates a presumption of access, but the right is

94. *Id.*; Rushford v. New Yorker Magazine, Inc., 846 F.2d 249, 253–54 (4th Cir. 1988).

95. *In re* United States, 707 F.3d at 291.

96. *Id.* at 290 (citing *Rushford*, 846 F.2d at 252).

97. *In re United States*, 707 F.3d at 290.

98. *See, e.g.*, Kinetic Concepts, Inc. v. Convatec Inc., 1:08CV00918, 2010 WL 1418312, at *9 (M.D.N.C. Apr. 2, 2010) ("the Fourth Circuit has used language that suggests that no public right of access attaches [to discovery motions]").

also not absolute.[99] The decision is made on a case-by-case basis.[100] The decision is left to the sound discretion of the district courts as required by *Nixon*, and the Fifth Circuit consistently requires district courts to explain decisions to seal or unseal a document.[101]

While there is a common law presumption in favor of public access, the Fifth Circuit does not characterize the public access presumption as "strong" or to require a strong showing of proof.[102]

The Fifth Circuit has not generally defined the term "judicial record."[103]

More recently, however, the Eastern District of Texas, in determining whether to grant the parties' unopposed motions to seal documents filed in connection with discovery motions, articulated three categories of court materials: (1) materials

---

99. S.E.C. v. Van Waeyenberghe, 990 F.2d 845, 848 (5th Cir. 1993); Belo Broad. Corp. v. Clark, 654 F.2d 423, 429 (5th Cir. 1981).

100. Vantage Health Plan, Inc. v. Willis-Knighton Med. Ctr., 913 F.3d 443, 450 (5th Cir. 2019) (citing United States v. Sealed Search Warrants, 868 F.3d 385, 390 (5th Cir. 2017)).

101. *Sealed Search Warrants*, 868 F.3d at 395; *e.g.*, *Van Waeyenberghe*, 990 F.2d at 849; United States v. Holy Land Found. for Relief and Dev., 624 F.3d 685, 690 (5th Cir. 2010).

102. *Vantage Health Plan*, 913 F.3d at 450; *see Belo*, 654 F.2d at 434 (holding that the presumption, "however gauged in favor of public access to judicial records" is only one of the interests to be weighed. This presumption applies so long as a document is a judicial record. *See Van Waeyenberghe,* 990 F.2d at 849.

103. *See* Bradley on behalf of AJW v. Ackal, 954 F.3d 225, 227 (5th Cir. 2020) (holding that sealed minutes are judicial records) (citing *In re United States*, 707 F.3d at 290 (stating that it is commonsensical that judicially authored or created documents are judicial records)); *Van Waeyenberghe*, 990 F.2d at 849 (holding that once a settlement agreement is filed in the district court, it becomes a judicial record).

that relate to dispositive issues in the case; (2) materials that relate to nondispositive issues in the case, and in particular, materials filed in connection with discovery disputes unrelated to the merits of the case; and (3) materials such as discovery that are exchanged between the parties and not made part of a court filing.[104] Under this framework, the court found that where materials relate to dispositive issues in a case, the party moving to seal the materials bears the burden to make a "compelling showing of particularized need to prevent disclosure."[105] On the other hand, the "good cause" standard of Rule 26(c) applies to materials that relate to nondispositive issues in the case, which includes materials filed in connection with discovery disputes unrelated to the merits of the case.[106] Finally, materials that are exchanged between the parties but not filed with the court are not subject to the public interest in open judicial proceedings.[107]

The Eastern District of Texas applied this framework in *Script Security Solutions, LLC v. Amazon.com, Inc.*[108] In *Script Security Solutions*, the defendant moved to redact confidential information from a hearing transcript but failed to satisfy either the "compelling showing of particularized need" standard or

104. Robroy Indus.-Tex., LLC v. Thomas & Betts Corp., No. 2:15-CV-512-WCB, 2016 WL 325174, at *2 (E.D. Tex. Jan. 27, 2016).

105. *Id*. (citing Ctr. for Auto Safety v. Chrysler Group, LLC, 809 F.3d 1092 (9th Cir. 2016)).

106. *Robroy* (citing Foltz v. State Farm Mut. Auto. Ins. Co., 331 F.3d 1122, 1135 (9th Cir. 2003); Leucadia, Inc. v. Applied Extrusion Techs., Inc., 998 F.2d 157, 164–65 (3d Cir. 1993); Anderson v. Cryovac, Inc., 805 F.2d 1, 13 (1st Cir. 1986)).

107. *Robroy* (citing Seattle Times Co. v. Rhinehart, 467 U.S. 20, 33 (1984)).

108. No. 2:15-CV-1030-WCB, 2016 WL 7013938, at *2 (E.D. Tex. Dec. 1, 2016).

the less-stringent "good cause" standard.[109] While the Eastern District of Texas cited *Center for Auto Safety v. Chrysler Group*[110] to support applying the "compelling reasons" standard to materials that relate to dispositive issues in the case, it did not specifically incorporate the Ninth Circuit's "tangentially related" language. *Center for Auto Safety* expressly rejected a mechanical application of the dispositive and nondispositive classifications as a way to decide which standard should apply to determine whether the documents should be sealed. However, it seems that the Eastern District of Texas still maintained the more rigid dispositive and nondispositive motion distinction, because the court in *Script Security Solutions* implied that it would incorporate the Ninth Circuit's less rigid distinctions when it said it would likely apply the "compelling reasons" test to the motion to redact portions of a hearing transcript.[111] This issue has not been fully addressed, however, as neither case has been heard by the Fifth Circuit, and thus this issue remains unsettled in the Fifth Circuit.[112]

6. Sixth Circuit

The Sixth Circuit recognizes that the long-established legal tradition under the common law of the presumptive right of the public to inspect and copy judicial documents and files goes back to the Nineteenth Century.[113] "Only the most compelling

109. *Id*.

110. 809 F.3d 1092, 1099 (9th Cir. 2016). See "Ninth Circuit," *infra*, for further discussion of *Center for Auto Safety*.

111. *Script Security Solutions*, 2016 WL 7013938, at *2.

112. *Id*.

113. *In re* Knoxville News-Sentinel Co, 723 F.2d 470, 474 (6th Cir. 1983) (quoting Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 597 (1978) and collecting cases).

reasons can justify non-disclosure of judicial records."[114] The Sixth Circuit has also recognized that the right of public access enjoyed under the First Amendment applies to civil proceedings.[115]

Although the Sixth Circuit has not explicitly defined "judicial record," district courts within the Sixth Circuit have cited the Second Circuit's *Lugosch v. Pyramid Co. of Onondaga*[116] decision that a judicial document is one that is "relevant to the performance of the judicial function and useful in the judicial process."[117]

Like other Circuits, the Sixth Circuit recognizes that the right to public access is "not absolute."[118] A party seeking to seal records must show that: (1) a compelling interest in sealing the records exists; (2) that the interest in sealing outweighs the public's interest in accessing the records; and (3) that the request is narrowly tailored.[119] "To do so, the party must 'analyze in detail, document by document, the propriety of secrecy, providing reasons and legal citations.'"[120] The party seeking to seal the records bears a "heavy" burden; simply showing that public disclosure of the information would, for instance, harm a

114. *In re Knoxville News*, 723 F.2d at 476.

115. Brown & Williamson Tobacco Corp. v. F.T.C., 710 F.2d 1165, 1177 (6th Cir. 1983) ("The Supreme Court's analysis of the justifications for access to the criminal courtroom apply as well to the civil trial.").

116. 435 F.3d 110, 119 (2d Cir. 2006).

117. *See, e.g.*, Snook v. Valley OB-GYN Clinic, P.C., 14-CV-12302, 2014 WL 7369904, at *2 (E.D. Mich. Dec. 29, 2014); Thompson v. Deviney Constr. Co., 216-CV-03019-JPM-DKV, 2017 WL 10662030, at *2 (W.D. Tenn. Dec. 15, 2017).

118. *In re Knoxville News*, 723 F.2d at 474 (quoting *Nixon*, 435 U.S. at 598).

119. Kondash v. Kia Motors Am., Inc., 767 F. App'x 635, 637 (6th Cir. 2019) (citation omitted).

120. *Id*. (citation omitted).

company's reputation is insufficient.[121] Instead, the moving party must show that it will suffer a "clearly defined and serious injury" if the judicial records are not sealed.[122]

When sealing court records, courts in the Sixth Circuit "must set forth specific findings and conclusions 'which justify nondisclosure to the public.'"[123] District courts must consider "each pleading [to be] filed under seal or with redactions and to make a specific determination as to the necessity of nondisclosure in each instance" and must "bear in mind that the party seeking to file under seal must provide a 'compelling reason' to do so and demonstrate that the seal is 'narrowly tailored to serve that reason.'"[124] If a district court "permits a pleading to be filed under seal or with redactions, it shall be incumbent upon the court to adequately explain 'why the interests in support of nondisclosure are compelling, why the interests supporting access are less so, and why the seal itself is no broader than necessary.'"[125] Moreover, the compelling reasons for nondisclosure of judicial documents must be expressly stated on the record.[126] Moreover, a party to an action cannot waive the public's First Amendment right to access.[127]

---

121. *Id.*; Shane Grp., Inc. v. Blue Cross Blue Shield of Mich., 825 F.3d 299, 305 (6th Cir. 2016).

122. *Id*. at 307.

123. Rudd Equip. Co., Inc. v. John Deere Constr. & Forestry Co., 834 F.3d 589, 594 (6th Cir. 2016) (citation omitted).

124. *In re* Nat'l Prescription Opiate Litig., 927 F.3d 919, 939–40 (6th Cir. 2019) (quoting *Shane Grp.*, 825 F.3d at 305).

125. *In re Nat'l Prescription Opiate Litig.*, 927 F.3d at 940 (quoting *Shane Grp.*, 825 F.3d at 306).

126. *Rudd Equip.*, 834 F.3d at 595 (citing Tri-Cty. Wholesale Distribs., Inc. v. Wine Grp., Inc., 565 F. App'x. 477, 490 (6th Cir. 2012)).

127. *Rudd Equip.*, 834 F.3d at 595.

7. Seventh Circuit

The Seventh Circuit recognizes both a common law and First Amendment right to inspect public records.[128]

"Judicial records" are "materials submitted to the court that 'affect the disposition' of the case and are not subject to a statute, rule, or privilege that justifies confidentiality."[129] This may include discovery material filed with the court that actually influences or underpins a judicial decision.[130] However, not every document filed with the court is part of the "judicial record."[131] Instead, the "judicial record" includes only materials that actually formed the basis of the parties' dispute and the district court's resolution.[132]

Courts weigh the First Amendment right of access, balancing the interests of the public against injury to the party seeking to seal judicial records, reconciling harm with newsworthiness.[133] The Seventh Circuit requires a showing of a "compelling interest in secrecy" to rebut the presumption of a right of access.[134] "The interest in secrecy is weighed against the

128. Courthouse News Serv. v. Brown, 908 F.3d 1063, 1068–69 (7th Cir. 2018), *cert. denied*, 140 S. Ct. 384 (2019).

129. United States v. Curry, 641 F. App'x. 607, 609 (7th Cir. 2016) (unpublished), quoting City of Greenville v. Syngenta Crop Protection, LLC, 764 F.3d 695, 697 (7th Cir. 2014).

130. Baxter Int'l., Inc., v Abbott Labs., 297 F.3d 544, 545 (7th Cir. 2002).

131. Goesel v. Boley Inter. (H.K.) Ltd., 738 F.3d 831, 833 (7th Cir. 2013).

132. *Id*. (quoting *Baxter*, 297 F.3d at 548).

133. Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1232 (7th Cir. 1993).

134. Jessup v. Luther, 277 F.3d 926, 928 (7th Cir. 2002) (citing Citizens First Nat'l Bank v. Cincinnati Ins. Co., 178 F.3d 943, 945 (7th Cir. 1999); Doe v. Blue Cross & Blue Shield United of Wis., 112 F.3d 869, 872 (7th Cir. 1997); Miller v. Indiana Hosp., 16 F.3d 549, 551 (3d Cir. 1994)).

competing interests case by case."[135] Additionally, a court may not solely rely on designations of confidentiality made by the parties.[136] Examples of a compelling interest in secrecy include trade secrets, the identity of informers, attorney-client privilege, state secrets, and the privacy of children.[137]

Even when a compelling interest in secrecy exists, courts must act with precision to seal as little information as necessary and are instructed to choose redactions rather than seal entire documents whenever possible.[138] However, the Seventh Circuit has contemplated that in cases involving "thousands of documents," there is no objection to a court crafting a broader order that seals information designated by the parties as highly sensitive if (1) the parties act in good faith in designating documents as confidential, and (2) any party or interested member of the public can challenge the order.[139]

8. Eighth Circuit

The Eighth Circuit recognizes a common law right to access records but has "not decided whether there is a First Amendment right of public access to the court file in civil

135. *Jessup*, 277 F.3d 926 (citing Cent. Nat'l Bank v. U.S. Dep't of Treasury, 912 F.2d 897, 900 (7th Cir. 1990)). This showing must be articulated on the record. *In re* Associated Press, 162 F.3d 503, 510 (7th Cir. 1998) ("upon entering orders which inhibit the flow of information between the courts and the public, district courts should articulate on the record their reasons for doing so," quoting Grove Fresh Distribs., Inc. v. Everfresh Juice Co., 24 F.3d 893, 898 (7th Cir. 1994)).

136. *See* Star Sci., Inc. v. Carter, 204 F.R.D 410, 416 (S.D. Ind. 2001); *see also Citizens First Nat'l Bank*, 178 F.3d at 945.

137. *Jessup*, 277 F.3d at 928; *see also* Mitze v. Saul, 968 F.3d 689, 692 (7th Cir. 2020).

138. *Mitze*, 968 F.3d at 692.

139. *Citizens First Nat'l Bank*, 178 F.3d at 946.

proceedings."[140] This common law right of access is not absolute; it "requires a weighing of competing interests."[141] A district court must balance "the degree to which sealing a judicial record would interfere with the interests served by the common-law right of access against the salutary interests served by maintaining confidentiality of the information sought to be sealed."[142] The weight afforded to the presumption of access is determined by role of the material at issue.[143]

While the Eighth Circuit has not explicitly defined the term "judicial record," the District of Minnesota has concurred with the Fourth and D.C. Circuits that judicial records are "documents that are relevant to and integrally involved in the resolution of the merits of a case."[144] Applying the principles from *Littlejohn v. BIC Corp.*,[145] the court in *Wood v. Robert Bosch Tool Corp*.[146] held that exhibits identified in the defendant's post-trial motion to seal were not judicial records and were protected from public access. In addition, the Third Circuit does not

140. IDT Corp. v. eBay, 709 F.3d 1220, 1224 (8th Cir. 2013).

141. Webster Groves Sch. Dist. v. Pulitzer Publ'g Co., 898 F.2d 1371, 1376 (8th Cir. 1990).

142. *IDT Corp.*, 709 F.3d at 1223.

143. *Id.*, at 1223–24.

144. Sorin Grp. USA, Inc. v. St. Jude Med. S.C., Inc., 14-CV-04023 (JRT/HB), 2019 WL 2107282, at *3 (D. Minn. May 14, 2019), quoting Krueger v. Ameriprise Fin., Inc., CV 11-2781 (SRN/JSM), 2014 WL 12597948, at *9 (D. Minn. Oct. 14, 2014), *aff'd*, 11-CV-02781 SRN/JSM, 2015 WL 224705 (D. Minn. Jan. 15, 2015).

145. 851 F.2d 673 (3rd Cir. 1988).

146. No. 4:13CV01888 PLC, 2016 WL 7013034, at *7 (E.D. Mo. Nov. 30, 2016).

appear to view nondispositive motions and exhibits to be included in the right of access.[147]

Unlike some circuits, the Eighth Circuit does not recognize a "strong presumption" of public access to judicial records.[148] Instead, the Eighth Circuit appears to defer to the judgment of the trial court.[149] Although the Eighth Circuit has not provided explicit guidance, district courts in the Circuit[150] have employed a six-factor test to determine whether a party has overcome the presumption in favor of publication: (1) the need to public access to the documents at issue; (2) the extent of previous public access to the documents; (3) the fact that someone has objected to disclosure, and the identity of that person; (4) the strength of any property and privacy interests asserted; (5) the possibility of prejudice to those opposing disclosure; and (6) the purposes for which the documents were introduced during the judicial proceedings.[151] The presumption of access is high when the

147. *See IDT Corp.*, 709 F.3d at 1223 (stating that "other than discovery motions and accompanying exhibits" the modern trend is to treat pleadings as presumptively public).

148. *In re* Bair Hugger Forced Air Warming Devices Prods. Liab. Litig., No. 15-MD-2666 (JNE/DTS), 2020 WL 4035548, at *1 (D. Minn. July 17, 2020) (quoting United States v. Webbe, 791 F.2d 103, 105 (8th Cir. 1986)).

149. Wood v. Robert Bosch Tool Corp., No. 4:13CV01888 PLC, 2016 WL 7013034, at *5 (E.D. Mo. Nov. 30, 2016) (quoting Webster Groves Sch. Dist. v. Pulitzer Publ'g Co., 898 F.2d 1371, 1376 (8th Cir. 1990).

150. For example, the District of Minnesota has found that the party seeking to have to information sealed must show that there is a "compelling reason" to overcome the public's right to access judicial records. Hudock v. LG Elecs. U.S.A., Inc., No. 0:16-CV-1220-JRT-KMM, 2020 WL 2848180, at *1 (D. Minn. June 2, 2020).

151. Bader Farms, Inc. v. Monsanto Co., No. 1:16-CV-00299-SNLJ, 2021 WL 289265, at *2 (E.D. Mo. Jan. 28, 2021); Nagel v. United Food & Comm. Workers Union, No. 18-CV-1053 (WMW/ECW), 2020 WL 6145111, at *2 (D. Minn.

judicial record may be used by the public "to evaluate the reasonableness and fairness of the judicial proceedings."[152]

9. Ninth Circuit

In the Ninth Circuit, a strong presumption of access, based in both the common law and the First Amendment, attaches to court records.[153] The presumption of access to judicial proceedings "flows from an 'unbroken, uncontradicted history rooted in the common law that justice must satisfy the appearance of justice.'"[154]

A "judicial document" is any item filed with a court that is "relevant to the judicial function and useful in the judicial process."[155] In the Ninth Circuit, this has been interpreted to exclude documents filed in connection with discovery matters. Documents obtained in discovery are treated differently. Despite its "strong preference for public access," "the right to inspect and copy judicial records is not absolute," and the Ninth Circuit has "carved out an exception" for sealed materials

---

Oct. 20, 2020); *see also* Sorin Grp. USA, Inc. v. St. Jude Med. S.C., Inc., 14-CV-04023 (JRT/HB), 2019 WL 2107282, at *3 (D. Minn. May 14, 2019) (quoting Doe v. Exxon Mobile Corp., 570 F. Supp. 2d 49, 52 (D.D.C. 2008) and United States v. Hubbard, 650 F.2d 293, 318 (D.C. Cir. 1980)).

152. *Sorin Grp.*, 2019 WL 2107282, at*4.

153. Courthouse News Serv. v. Planet, 947 F.3d 581, 589 (9th Cir. 2020) ("We have long presumed a First Amendment 'right of access to court proceedings and documents'"); *see also* Ctr. for Auto Safety v. Chrysler Grp., LLC, 809 F.3d 1092, 1098, 1101 (9th Cir. 2016); Foltz v. State Farm Mut. Auto. Ins. Co., 331 F.3d 1122, 1135 (9th Cir. 2003) ("Following the Supreme Court's lead, 'we start with a strong presumption of access to court records.'").

154. *Courthouse News*, 947 F.3d at 589 (quoting Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 573–74 (1980)).

155. *Courthouse News*, 947 F.3d at 592 (citing *Judicial Document*, BLACK'S LAW DICTIONARY (10th ed. 2014)).

attached to a discovery motion unrelated to the merits of a case.[156] Under this exception, a party need only to satisfy the less exacting "good cause" standard from Rule 26(c)(1) to seal such documents from public view.[157]

On the other hand, a party seeking to seal a judicial record bears the burden of overcoming the strong presumption of access by meeting the "compelling reasons" standard, a "stringent standard" that permits sealing only when a court finds a compelling reason and articulates the factual basis for the ruling, without relying on hypothesis or conjecture.[158] What constitutes a "compelling reason" is "best left to the sound discretion of the trial court."[159]

As an extension of these principles, when deciding what test to apply to a motion to *unseal* a particular court filing—the presumptive "compelling reasons" standard or the "good cause" exception—the Ninth Circuit has "sometimes deployed the terms 'dispositive' and 'non-dispositive,'" referring to the type of motion to which the documents are appended. However, in the wake of *Center for Auto Safety*, the Ninth Circuit expressly rejects a mechanical application of the dispositive and nondispositive classifications as a means of deciding which standard should apply to determine whether documents should be sealed. Rather, considerations of the public's right of access turns on "whether the [underlying] motion is more than

156. *Ctr. for Auto Safety*, 809 F.3d at 1096–97 (quoting Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 598 (1978)).

157. *Ctr. for Auto Safety*, 809 F.3d at 1097 (citing Seattle Times Co. v. Rhinehart, 467 U.S. 20, 33 (1984) and Anderson v. Cryovac, Inc., 805 F.2d 1, 13 (1st Cir. 1986)).

158. *Ctr. for Auto Safety*, 809 F.3d at 1096–97 (quoting Kamakana v. City & Cnty. of Honolulu, 447 F.3d 1172, 1178 (9th Cir. 2006).

159. *Ctr. for Auto Safety*, 809, F.3d at 1097 (quoting *Nixon*, 435 U.S. at 599).

tangentially related to the merits of a case."[160] This standard provides necessary flexibility, because some nondispositive motions, such as motions in limine, "are strongly correlative to the merits of a case," and thus warrant application of the higher standard to seal.[161] Such balancing also allows the court to recognize the "special role" that protective orders play. It does not make sense to render a district court's protective order useless simply because a party attached a sealed discovery document to a nondispositive motion.[162] In such circumstances, the "good cause" standard to seal applies.[163]

10. Tenth Circuit

The Tenth Circuit recognizes a common law right of access to judicial records.[164] The Tenth Circuit, however, has repeatedly declined to address whether a First Amendment right of access exists for civil trials.[165]

---

160. *Ctr. for Auto Safety*, 809 F.3d at 1099.

161. *Id*.

162. *Id*. at 1097–98.

163. *Id*. *Compare with* Foltz v. State Farm Mut. Auto. Ins. Co., 331 F.3d 1122, 1135–36 (9th Cir. 2003), in which the Ninth Circuit applied the "compelling reasons" test as to whether documents attached to a motion for summary judgment should be sealed; *see also Kamakana*, 447 F.3d at 1178–80.

164. Mann v. Boatright, 477 F.3d 1140, 1149 (10th Cir. 2007).

165. Parson v. Farley, 352 F. Supp. 3d 1141, 1152, n. 5 (N.D. Okla. 2018), *aff'd*, No. 16-CV-423-JED-JFJ, 2018 WL 6333562 (N.D. Okla. Nov. 27, 2018); United States v. McVeigh, 119 F.3d 806, 814 (10th Cir. 1997); United States v. Roberts, 88 F.3d 872, 882–83 (10th Cir. 1996). *But see* Angilau v. United States, No. 2:16-00992-JED, 2017 WL 5905536, at *8 (D. Utah Nov. 29, 2016), *aff'd*, No. 216CV00992JEDPJC, 2018 WL 1271894 (D. Utah Mar. 9, 2018) (contested documents that have been submitted as supporting material in connection with motions for summary judgment are considered judicial documents under the common law and there is a qualified "First Amendment right of access to documents submitted to the court in connection with a summary judgment

Aligning with most circuits, the Tenth Circuit considers the interest of the public in judicial proceedings as "presumptively paramount."[166] To overcome this presumption, a party must establish that disclosure "will work a clearly defined and serious injury."[167] "'[T]he parties must articulate a real and substantial interest that justifies depriving the public of access to the records that inform our decision-making process.'"[168]

In the Tenth Circuit, a qualified right of public access applies to judicial documents.[169] Although what constitutes a "judicial document" is not clearly defined, the Tenth Circuit has positively cited the Second Circuit's *Lugosch* decision, which found that merely filing a document with the court is insufficient; rather, "where documents are used to determine litigants' substantive legal rights, a strong presumption of access attaches."[170] It has also cited favorably to the D.C. Circuit's *United States v. El-Sayegh* case[171] that "what makes a document a judicial

motion." *See also* Brigham Young Univ. v. Pfizer, Inc., 281 F.R.D. 507, 511 (D. Utah 2012) (quoting Lugosch v. Pyramid Co. of Onondaga, 435 F.3d 110, 124 (2d Cir. 2006).

166. Crystal Grower's Corp. v. Dobbins, 616 F.2d 458, 461 (10th Cir. 1980) (citing Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 602 (1978)).

167. Harte v. Burns, No. 13-2586-JWL, 2020 WL 1888823, at *2 (D. Kan. Apr. 16, 2020); United States v. Walker, 761 F. App'x. 822, 834 (10th Cir. 2019); Eugene S. v. Horizon Blue Cross Blue Shield of N.J., 663 F.3d 1124, 1135–36 (10th Cir. 2011).

168. Colony Ins. Co. v. Burke, 698 F.3d 1222, 1242 (10th Cir. 2012) (quoting Helm v. Kansas, 656 F.3d 1277, 1292 (10th Cir. 2011)).

169. *Angilau*, 2017 WL 5905536, at *7; *see also Colony Ins. Co.*, 698 F.3d at 1241 (quoting Soc'y of Prof'l Journalists v. Secretary of Labor, 616 F. Supp. 569, 576 (D. Utah 1985), *appeal dismissed*, 832 F.2d 1180 (10th Cir. 1987)).

170. *Colony Ins. Co.*, 698 F.3d at 1242 (quoting *Lugosch*, 435 F.3d at 121).

171. 131 F.3d 158, 163 (D.C.Cir. 1997).

record . . . is the role it plays in the adjudicatory process."[172] While pretrial documents and discovery materials that the parties intended to keep confidential may be sealed, agreement alone cannot support sealing.[173]

11. Eleventh Circuit

The Eleventh Circuit recognizes both a common law right and a limited First Amendment right of access to civil trial proceedings.[174]

Under common law, a trial court concealing the entire record of a case must show that "the denial [of access] is necessitated by a compelling governmental interest, and is narrowly tailored to that interest."[175] When concealing particular documents of a case, the court must balance the competing interests of the parties.[176] Public access to civil documents and proceedings receives less First Amendment protection, and "[m]aterials merely gathered as a result of the civil discovery process . . . do not fall within the scope of the constitutional right of access's compelling interest standard."[177] Rather, in determining whether to unseal the discovery materials, the First Amendment

172. *See* United States v. Apperson, 642 F. App'x. 892, 899 n. 6 (10th Cir. 2016) (unpublished).

173. Grundberg v. Upjohn Co., 140 F.R.D. 459, 466 (D. Utah 1991); Sacchi v. IHC Health Servs., Inc., 918 F.3d 1155, 1160 (10th Cir. 2019).

174. Chicago Tribune Co. v. Bridgestone/Firestone, Inc., 263 F.3d 1304, 1311 (11th Cir. 2001) (per curiam).

175. *Id*. at 1311 (quoting Wilson v. Am. Motors Corp., 759 F.2d 1568, 1571 (11th Cir. 1985)).

176. *Chicago Tribune*, 263 F.3d at 1311.

177. *Id*. at 1310.

right of access standard is "identical to the Rule 26 good cause standard."[178]

In the Eleventh Circuit, "the mere filing of a document does not transform it into a judicial record."[179] Rather, judicial documents are those that are "integral to the 'judicial resolution of the merits' in any action taken by that court."[180] When a document is filed, the type of filing to which it is attached is a factor for the court to consider in deciding whether the document constitutes a judicial record.[181] For instance, documents filed in connection with discovery motions are not considered judicial documents and are not subject to the common law right of access.[182] However, discovery materials filed in connection with pretrial motions that require judicial resolution of the merits are subject to the common law right.[183] Any "motion that is 'presented to the court to invoke its powers or affect its decisions,' whether or not characterized as dispositive, is subject to the public right of access."[184]

---

178. *Id*. (finding error in requiring a party to show a compelling interest to overcome the public's constitutional right of access).

179. Comm'r., Alabama Dept. of Corrections v. Advance Local Media, LLC, 918 F.3d 1161, 1167 (11th Cir. 2019).

180. *Id*.; F.T.C. v. AbbVie Prod. LLC, 713 F.3d 54, 64 (11th Cir. 2013); *Chicago Tribune*, 263 F.3d at 1312.

181. *Advance Local Media*, 918 F.3d at 1166–68.

182. *Chicago Tribune*, 263 F.3d at 1313; *In re* Alexander Grant & Co. Litig., 820 F.2d 352, 355 (11th Cir. 1987).

183. *Chicago Tribune*, 263 F.3d at 1312 (the court distinguishes between material filed with discovery motions and material filed in connection with more substantive procedures); Romero v. Drummond Co., Inc., 480 F.3d 1234, 1245 (11th Cir. 2007) (presumption applies to "material filed in connection with pretrial motions that require judicial resolution of the merits" but not documents "filed in connection with motions to compel discovery").

184. *Id*. at 1246 (citing United States v. Amodeo (*Amodeo II*), 71 F.3d 1044, 1050 (2d Cir. 1995).

12. D.C. Circuit

Relying on the Ninth Circuit's decision in *Foltz v. State Farm Mutual Auto Insurance Co.*,[185] the D.C. Circuit recognizes a common law right of access to judicial records.[186] Further, the First Amendment "guarantees the press and the public access to aspects of court proceedings, including documents, 'if such access has historically been available, and serves an important function of monitoring prosecutorial or judicial misconduct[.]'"[187] The D.C. Circuit applies the *Press-Enterprise II* test to determine if the sealed records have "historically been available, and serves an important function of monitoring prosecutorial or judicial misconduct."[188] However, it is unclear whether the First Amendment right to access applies in civil cases.[189]

In the D.C. Circuit, "not all documents filed with courts are judicial records."[190] What makes a document a "judicial record" is "the role it plays in the adjudicatory process."[191] The reason for this rule is intuitive: "the concept of a judicial record assumes a judicial decision, and with no such decision, there is nothing judicial about the record."[192] The common law right of access does not apply to documents "whose contents were not

185. 331 F.3d 1122 (9th Cir. 2003).

186. Apple Inc. v. Samsung Electronics Co., 727 F.3d 1214 (D.C. Cir. 2013).

187. S.E.C. v. Am. Int'l Grp., 712 F.3d 1, 5 (D.C. Cir. 2013).

188. Washington Post v. Robinson, 935 F.2d 282, 288 (D.C. Cir. 1991) (citing Press-Enterprise. Co. v. Superior Court of Calif. For Riverside Cty. (*Press-Enterprise II*), 478 U.S. 1, 8 (1986); Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 605–06 (1982); Oregonian Pub. Co. v. Dist. Court, 920 F.2d 1462, 1465 (9th Cir. 1990); United States v. Haller, 837 F.2d 84, 86 (2d Cir. 1988); *In re* Washington Post Co., 807 F.2d 383, 390 (4th Cir. 1986)).

189. *Am. Int'l Grp.*, 712 F.3d at 5.

190. *Id*. at 3.

191. *Id*.; United States v. El-Sayegh, 131 F.3d 158, 163 (D.C. Cir. 1997).

192. *Am. Int'l Grp.*, 712 F.3d at 3.

specifically referred to or examined upon during the course of those proceedings and whose only relevance to the proceedings derived from the defendants' contention that many of them were not relevant to the proceedings . . . ."[193]

"A party seeking to seal judicial records can overcome the strong presumption of access by providing 'sufficiently compelling reasons' that override the public policies favoring disclosure."[194] Such compelling reasons must be "supported by specific factual findings that outweigh the general history of access and the public policies favoring disclosure, such as the public interest in understanding the judicial process."[195] This requires courts in the D.C. Circuit to "conscientiously balance the competing interests of the public and the party who seeks to keep certain judicial records secret."[196]

Under the common law analysis, courts in the D.C. Circuit consider six factors relating to the generalized interests for and against public disclosure, which "can be weighed without examining the contents of the documents at issue[]," but instead looks to the role the document plays in the litigation.[197] Those factors include: (1) the need for public access to the documents at issue; (2) previous public access to the documents; (3) the fact of an objection to public access and the identity of those objecting to public access; (4) the strength of the generalized property

193. United States v. Hubbard, 650 F.2d 293, 316 (D.C. Cir. 1980).

194. Apple Inc. v. Samsung Electronics Co., 727 F.3d 1214, 1221 (D.C. Cir. 2013) (citing *In re* Midland Nat'l Life Ins. Co. Annuity Sales Practices Litig., 686 F.3d 1115, 1119 (9th Cir. 2012) (quoting Foltz v. State Farm Mut. Auto. Ins. Co., 331 F.3d 1122, 1135 (9th Cir. 2003)).

195. *Apple*, 727 F.3d at 1221 (citing Kamakana v. City & Cty. of Honolulu, 447 F.3d 1172, 1178–79 (9th Cir. 2006) (alterations and internal quotation marks omitted)).

196. *Kamakana*, 447 F.3d at 1179.

197. *Hubbard*, 650 F.2d at 317.

and privacy interests asserted; (5) the possibility of prejudice; and (6) the purposes for which the documents were introduced.[198] The proponent of a motion to seal must demonstrate that these six factors, in totality, overcome the "strong presumption in favor of public access to judicial proceedings," which is "the starting point in considering a motion to seal court records."[199]

198. *Id*. at 317–22.

199. E.E.O.C. v. Nat'l Children's Ctr., 98 F.3d 1406, 1409 (D.C. Cir. 1996) (quoting Johnson v. Greater Se. Cty. Hosp. Corp., 951 F.2d 1268, 1277 (D.C.Cir. 1991)).

ATTACHMENT A: OVERVIEW OF JUDICIAL RECORD DEFINITION BY CIRCUIT

Circuit	Judicial Record Defined?
First	Yes. "[M]aterials on which a court relies in determining the litigants' substantive rights" *In re Providence Journal*, 293 F.3d 1, 9–10 (1st Cir. 2002), quoting *Anderson v. Cryovac, Inc*., 805 F.2d 1, 13 (1st Cir. 1986).
Second	Yes. Information that is "relevant to the performance of the judicial function and useful in the judicial process." *Lugosch v. Pyramid Co. of Onondaga*, 435 F.3d 110, 119 (2d Cir. 2006).
Third	Yes. A document that "has been filed with the court . . . or otherwise somehow incorporated or integrated into a district court's adjudicatory proceedings." *In re Avandia Mktg., Sales Practices & Prod. Liab. Litig*., 924 F.3d 662, 672–73 (3d Cir. 2019).
Fourth	Yes. Documents filed with the court that "play a role in the adjudicative process, or adjudicate substantive rights." *In re Application of the United States for an Order Pursuant to 18 U.S.C. Section 2703(D),* 707 F.3d 283, 290 (4th Cir. 2013).
Fifth	Not specifically. *See Bradley on behalf of AJW v. Ackal*, 954 F.3d 216, 227 (5th Cir. 2020) (court has not generally defined "judicial record," but it is common sense that judicially authored or created documents are judicial records).

Circuit	Judicial Record Defined?
Sixth	Not specifically. However, district courts cite favorably to Second Circuit's *Lugosch* decision that a judicial document is one that is "relevant to the performance of the judicial function and useful to in the judicial process." *See, e.g., Snook v. Valley OB-GYN Clinic, P.C.*, 14-CV-12302, 2014 WL 7369904, at *2 (E.D. Mich. Dec. 29, 2014); *Thompson v. Deviney Constr. Co., Inc.*, 216CV03019JPMDKV, 2017 WL 10662030, at *2 (W.D. Tenn. Dec. 15, 2017).
Seventh	Yes. "[M]aterials submitted to the court that 'affect the disposition' of the case and are not subject to a statute, rule, or privilege that justifies confidentiality." *United States v. Curry*, 641 F. App'x. 607, 609 (7th Cir. 2016) (unpublished), quoting *City of Greenville v. Syngenta Crop Protection*, LLC, 764 F.3d 695, 697 (7th Cir. 2014).
Eighth	No. However, the District of Minnesota has concurred with the Fourth and D.C. Circuits that judicial records are "documents that are relevant to and integrally involved in the resolution of the merits of a case[.]" *Sorin Grp. USA, Inc. v. St. Jude Med. S.C., Inc.*, 14-CV-04023 (JRT/HB), 2019 WL 2107282, at *3 (D. Minn. May 14, 2019), quoting *Krueger v. Ameriprise Fin., Inc.*, CV 11-2781 (SRN/JSM), 2014 WL 12597948, at *9 (D. Minn. Oct. 14, 2014), aff'd, 11-CV-02781 SRN/JSM, 2015 WL 224705 (D. Minn. Jan. 15, 2015).

Circuit	Judicial Record Defined?
Ninth	Yes. Any item filed with a court that is "relevant to the judicial function and useful in the judicial process." *Courthouse News Service v. Planet*, 947 F.3d 581 (9th Cir. 2020).
Tenth	No. But the Tenth Circuit has cited favorably to the Second Circuit's *Lugosch* decision, which found that a judicial document must be "relevant to the performance of the judicial function and useful in the judicial process." *See Colony Ins. Co. v. Burke*, 698 F.3d 1222, 1242 (10th Cir. 2012). It has also cited favorably to the D.C. Circuit's *El-Sayegh* case that "what makes a document a judicial record . . . is the role it plays in the adjudicatory process." *See United States v. Apperson*, 642 F. App'x. 892, 899 n. 6 (10th Cir. 2016) (unpublished).
Eleventh	Yes. Those that are "integral to the 'judicial resolution of the merits' in any action taken by that court." *Comm'r., Alabama Dept. of Corrections v. Adv. Loc. Media, LLC*, 918 F.3d 1161, 1167 (11th Cir. 2019) (citing *F.T.C. v. AbbVie Prod. LLC*, 713 F.3d 54, 64 (11th Cir. 2013) (quoting *Chicago Tribune Co. v. Bridgestone/Firestone, Inc.*, 263 F.3d 1304, 1312 (11th Cir. 2001).

Circuit	Judicial Record Defined?
D.C.	Yes. What makes a document a "judicial record" is the role it plays in the adjudicatory process. *United States v. El–Sayegh*, 131 F.3d 158, 163 (D.C. Cir. 1997). It must be specifically mentioned during the proceedings. *United States v. Hubbard*, 650 F.2d 293, 316 (D.C. Cir. 1980).

ATTACHMENT B: CIRCUIT ANALYSIS OF WHETHER PUBLIC RIGHT OF ACCESS EXISTS FOR NONDISPOSITIVE MOTIONS

Circuit	**Nondispositive-related Motions and Exhibits Included in Right of Access?**
First	No. *See United States v. Kravetz*, 706 F.3d 47, 54 (1st Cir. 2013) (no public right of access to discovery motions and related materials); *Anderson v. Cryovac, Inc.*, 805 F.2d 1, 13 (1st Cir. 1986) (a request to compel or protect the disclosure of information in the discovery process is not a request for a disposition of substantive rights).
Second	Unlikely. *Brown v. Maxwell*, 929 F.3d 41, 50 (2d Cir. 2019) ("The presumption of public access in filings submitted in connection with discovery disputes or motions in limine is generally somewhat lower than the presumption applied to material introduced at trial, or in connection with dispositive motions such as motions for dismissal or summary judgment.").
Third	Yes. *In re Avandia Mktg., Sales Practices & Prod. Liab. Litig.*, 924 F.3d 662, 672–73 (3d Cir. 2019).

Circuit	**Nondispositive-related Motions and Exhibits Included in Right of Access?**
Fourth	Unclear. *In re Application for an Order Pursuant to 18 U.S.C. Section 2703(D)*, 707 F.3d 283, 290 (4th Cir. 2013). But some district courts have predicted that the Fourth Circuit will find no public right of access to discovery motions and related exhibits, and that consequently, such documents may be sealed. *See, e.g.*, *Kinetic Concepts, Inc. v. Convatec Inc.*, 1:08tCV00918, 2010 WL 1418312, at *9 (M.D.N.C. Apr. 2, 2010) ("the Fourth Circuit has used language that suggests that no public right of access attaches [to discovery motions]").
Fifth	Unlikely. *Robroy Indus.-Tex., LLC v. Thomas & Betts Corp.*, No. 2:15-CV-512-WCB, 2016 WL 325174, at *2 (E.D. Tex. Jan. 27, 2016).
Sixth	Likely. A party seeking to seal records must advance arguments that allow the court to "set forth specific findings and conclusions 'which justify nondisclosure to the public.'" *Rudd Equip. Co., Inc. v. John Deere Constr. & Forestry Co.*, 834 F.3d 589, 594 (6th Cir. 2016).

Circuit	Nondispositive-related Motions and Exhibits Included in Right of Access?
Seventh	Depends. Public access depends on whether a document "influenc[ed] or underpin[ned] the judicial decision." *Baxter Int'l, Inc. v. Abbott Labs.,* 297 F.3d 544, 545 (7th Cir. 2002); *Matter of Cont'l Illinois Sec. Litig.*, 732 F.2d 1302, 1309 (7th Cir. 1984) (declining to comment as a general matter whether there is a recognized right of public access to pretrial proceedings but finding presumption does apply to a motion to terminate).
Eighth	No. *IDT Corp. v. eBay,* 709 F.3d 1220, 1223 (8th Cir. 2013) (stating that "other than discovery motions and accompanying exhibits," the modern trend is to treat pleadings as presumptively public).
Ninth	Possibly. Will turn on whether the motion is "more than tangentially related to the merits of the case[.]" *Ctr. for Auto Safety v. Chrysler Grp., LLC,* 809 F.3d 1092, 1098, 1101 (9th Cir. 2016).

Circuit	Nondispositive-related Motions and Exhibits Included in Right of Access?
Tenth	Likely at common law. *Parson v. Farley*, 352 F. Supp. 3d 1141, 1153 (N.D. Okla. 2018), aff'd, 16-CV-423-JED-JFJ, 2018 WL 6333562 (N.D. Okla. Nov. 27, 2018) (finding Motion to Dismiss and exhibit as "judicial documents."). Unlikely under the First Amendment. A "'litigant has no First Amendment right of access to information made available only for purposes of trying his suit' and that 'pretrial depositions and interrogatories are not public components of a civil trial.'" *Grundberg v. Upjohn Co.*, 140 F.R.D. 459, 466 (D. Utah 1991) (quoting *Seattle Times v. Rhinehart*, 467 U.S. 20, 32–33 (1984)).
Eleventh	Depends. *Romero v. Drummond Co., Inc.*, 480 F.3d 1234, 1245 (11th Cir. 2007) (presumption applies to "material filed in connection with pretrial motions that require judicial resolution of the merits" but not documents "filed in connection with motions to compel discovery").
D.C.	No. S*.E.C. v. Am. Int'l Grp.*, 712 F.3d 1, 3–4 (D.C. Cir. 2013) (presumption applies only to record that "plays a role in the adjudicatory process," not to documents where the court "ma[kes] no decisions about them or that otherwise relie[s] on them").

THE SEDONA CONFERENCE COMMENTARY ON CROSS-BORDER PRIVILEGE ISSUES

A Project of The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6)

Author:

The Sedona Conference

Editor-in-Chief:

Nichole Sterling

Contributing Editors:

Jordan W. Cowman — Huw Edwards

Karen O. Hourigan — Sean Lynch

William D. Marsillo — Todd Presnell

The Hon. Mr. Justice Elliott Myers

Steering Committee Liaison:

Jeane A. Thomas

Staff editors:

David Lumia — Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 6. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of

the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

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, *Commentary on Cross-Border Privilege Issues,* 23 SEDONA CONF. J. 475 (2022).

PREFACE

Welcome to the July 2022 final version of The Sedona Conference *Commentary on Cross-Border Privilege Issues* ("*Commentary*"), a project of The Sedona Conference Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG6 is to develop principles, guidance and best practice recommendations for information governance, discovery and disclosure involving cross-border data transfers related to civil litigation, dispute resolution and internal and civil regulatory investigations.

The Sedona Conference acknowledges Editor-in-Chief Nichole Sterling for her leadership and commitment to the project. We also thank Contributing Editors Jordan Cowman, Conor Crowley, Huw Edwards, Karen Hourigan, Sean Lynch, Bill Marsillo, Mr. Justice Elliott Myers, and Todd Presnell for their efforts, and Jeane Thomas for her guidance and input as Steering Committee liaison to the drafting team.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG6 who reviewed, commented on, and proposed edits to early drafts of the *Commentary* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG6 meetings where drafts of this *Commentary* were the subject of the dialogue. The publication was also subject to a period of public comment. On behalf of The

Sedona Conference, I thank both the membership and the public for all of their contributions to the *Commentary*.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG6 and several other Working Groups in the areas of electronic document management and discovery, data security and privacy liability, international data transfers, patent litigation, patent remedies and damages, and trade secrets.

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. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
July 2022

TABLE OF CONTENTS

I. INTRODUCTION[1]

Protections that limit discovery of documents and information under doctrines such as attorney-client privilege[2] and the work-product doctrine[3] vary from country to country. The differences are greatest between common law and civil law jurisdictions, reflecting material differences in the scope of discovery between these jurisdictions. This *Commentary* provides an overview[4] of select laws and the differences between them and sets forth practice points to consider in managing and resolving the conflicts that can arise in multijurisdictional matters where the protections afforded in one jurisdiction may not be

---

1. The Drafting Team for this *Commentary* would in particular like to thank the following individuals for their assistance and thoughtful comments during the drafting process: Francesca Rogo and Priyanka Surapaneni, Associates, Baker & Hostetler LLP in New York, New York; Franziska Fuchs, Robert Bosch GmbH in Stuttgart, Germany, and Jerry Johnson, Robert Bosch LLC in Farmington, Michigan; Natascha Gerlach, Director of EU Privacy and Data Policy, The Centre for Information Policy Leadership in Brus-sels, Belgium; Evelien Jamaels, Counsel, and Blanch Devos, Associate, Crow-ell & Moring LLP in Brussels, Belgium; Jared Weir, Associate, Greenberg Traurig LLP in Dallas, Texas; and Madeline MacDonald, former Clerk at the Supreme Court of British Columbia (currently at Harris and Company LLP in Vancouver, Canada).

2. The "attorney-client privilege" is referred to as "legal professional privilege," "client legal privilege," "legal advice privilege," and similar names in other jurisdictions. For purposes of this *Commentary*, "attorney-client privilege" is generally used to include all similar concepts, though differences in how those concepts are interpreted or applied in various jurisdictions are discussed as relevant. When other terms are used in this *Commentary*, it is for jurisdiction-specific reasons.

3. While recognizing that distinctions do exist between, for example, the U.S. work-product doctrine and the U.K. litigation privilege, we will use work-product doctrine generally throughout to refer to all similar concepts for protecting documents, unless a specific distinction is helpful.

4. A more detailed explanation of key laws discussed in various exemplar jurisdictions can be found in Appendix A.

recognized in, or may be in conflict with, those of another.[5] In our increasingly global world, multijurisdictional conflicts (and their attendant privilege issues) are becoming more common. Situations that counsel might encounter include:

- Producing documents and information during U.S. discovery that have been collected from custodians in various international jurisdictions with divergent privilege and disclosure protections.
- Voluntary disclosure of documents for regulatory compliance (or good will) in one jurisdiction that can lead to a privilege waiver in the courts of other jurisdictions during subsequent litigation.
- Protecting privilege in cross-border investigations that include the collection and review of (often sensitive) information and conducting employee interviews in multiple foreign jurisdictions before issuing an investigation report, which may be subject to compelled disclosure in certain jurisdictions.
- The conclusion of a litigation in one jurisdiction that is followed by a subsequent litigation in another jurisdiction, in which parties seek

5. The U.S. court system as well as the court systems of many other countries are divided into federal (national) courts and state courts. This *Commentary* focuses generally on national-level rules and decisions regarding privilege. We note there are a number of rules at the state level in the United States and elsewhere that may need to be consulted, depending on the particulars of a given situation. In the United States, most litigation involving parties from other countries will take place in federal courts under diversity jurisdiction.

> the production of previously produced documents and information, and the application of the same privilege determinations, despite significant jurisdictional differences in applicable privileges.

To understand the policies that shape the evidentiary and confidentiality protections that exclude documents and information from discovery in different jurisdictions, it is first helpful to understand the general scope of permitted discovery in the jurisdictions of interest. At a high level, civil procedure rules in common law jurisdictions typically permit parties to obtain nonprivileged documents and information relevant to their asserted claims and defenses from opposing parties and third parties. The scope of discovery within common law jurisdictions varies and, though not unlimited, can be quite broad, particularly in the United States.[6] Therefore, parties and courts will expect that any relevant documents and information will be produced. As a result, assertions of privilege and other protections to limit or preclude disclosure of requested documents and information are critical in many cases and are regularly disputed.

By contrast, in civil law countries, the scope of discovery is significantly narrower, and disputes concerning privilege, confidentiality, and other document protections are correspondingly less common. Discovery in most civil law countries is limited to the documents or information a party wants to rely upon to support its own case. Plaintiffs typically must support their cases with publicly available documents or information already

6. For example, U.S. courts, upon a party's request, may enter a protective order limiting or precluding the discovery of certain documents or information due to substantive reasons or the burden on the producing party. U.S. courts also may narrow or prohibit discovery that is duplicative, broader than necessary, seeks information of which the cost outweighs its benefit to the proceeding, or seeks confidential and proprietary information.

in their possession. Parties in many civil law countries may request orders from the court requiring another party to disclose a particular document, but these are limited disclosures. Jurisdictions vary as to how amenable courts are to such requests and the evidence required to support a successful request, effectively limiting such disputes.

Section II of this *Commentary* broadly explains the distinctions between common law and civil law privilege and other legal protections against disclosure. Section III lays out practical considerations for navigating these differences. Section IV explores the choice-of-law analysis used by some courts for deciding the application of privilege laws. Section V provides an appendix of privilege and other legal protections in selected exemplar jurisdictions.

II. PRIVILEGE AND OTHER LEGAL PROTECTIONS AGAINST DISCLOSURES

A. Common Law Privilege and Other Legal Protections

Common law jurisdictions generally protect documents and information falling within the scope of the attorney-client privilege or the work-product doctrine. As the name implies, the attorney-client privilege covers communications between a lawyer and client, including in-house counsel on behalf of the corporate employer client, in the context of seeking or providing legal advice. The work-product doctrine protects information gathered, created, or prepared, by or for counsel, for the purposes of litigation, whether anticipated or actual.[7] Notably, in some common law jurisdictions, such as Canada and the United States, the work-product doctrine does not require the involvement of counsel.[8] Additionally, the common-interest (or joint-

7. Note that U.S. courts vary as to the degree of motivation required to demonstrate that a document was prepared in anticipation of litigation. A majority of the federal circuit courts use a "because of" test, looking to whether the document was created because of the anticipated litigation. Other federal circuit courts use a "primary motivation" test whereby the primary motivating factor for the creation of the document is the anticipation of litigation. What qualifies as a litigation is also broad in the United States, and most courts will define any adversarial proceedings as falling within the scope of litigation for work-product protection. For further information on what can be considered anticipation of litigation for the purposes of implementing legal holds, which can inform whether work product applies, see The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341 (2019).

8. Blank v. Canada, [2006] S.C.C. 39 (Can.); Lizotte v. Aviva Ins. Co. of Can., [2016] S.C.C. 52 (Can.); United States v. Am. Tel. & Tel., 642 F.2d 1285 (D.C. Cir. 1980).

defense) doctrine,[9] while not uniform in its application, generally holds that a party does not waive the attorney-client privilege or work-product protection by sharing protected information with another party with whom it shares a common legal interest.[10]

Any common law privilege or protection can be waived explicitly or implicitly. The recognition of privilege or the loss of it in another jurisdiction outside the forum is largely governed by rules established by the courts.

1. Fundamental Tenets of the Common Law Attorney-Client Privilege

The attorney-client privilege is the oldest of the common law privileges, and aspects of this privilege can be detected in Roman law. Grounded in traditional concepts of honor, the attorney-client privilege has been well established in English law since the sixteenth century.[11] The attorney-client privilege in the United States and other common law jurisdictions covers confidential communications between a client and the client's attorney regarding legal advice. In the United States, the United Kingdom, and most other common law jurisdictions, the privilege can extend to licensed in-house counsel acting in a legal

9. This *Commentary* recognizes the distinctions between the common-interest and joint-defense doctrines but generally finds it easiest to discuss the two together.

10. To maintain the common-interest or joint-defense privilege in sharing communications with others, a party must typically demonstrate (1) that the communications were made pursuant to a joint defense or common interest of the parties; (2) that the communications were made to further the goals of that joint defense or common interest; and (3) that the privilege was not otherwise waived (i.e., that the joint defenders are not sharing the communications beyond their limited group).

11. EDNA SELAN EPSTEIN, 2 THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK-PRODUCT DOCTRINE (4th ed. 2001).

capacity. The attorney-client privilege is the foundation of the legal profession in common law countries, encouraging open and honest conversations between the client and the attorney without fear of disclosure, which in turn enables the attorney to provide sound legal advice.[12] The attorney-client privilege underpins the work done by attorneys practicing in common law jurisdictions on a daily basis, whether that work is related to litigation, business transactions, or other advice given by legal counsel, but this privilege can easily be lost if not protected.[13]

While each jurisdiction may have different requirements for creating and maintaining the attorney-client privilege, generally the elements of establishing the attorney-client privilege are:[14]

1. A confidential communication
2. between an attorney and a client
3. for the purpose of giving or receiving legal advice
4. when the privilege has not otherwise been waived.

We explore each of these elements and other related considerations in the Sections that follow.

---

12. Jackie Unger, *Maintaining the Privilege: A Refresher on Important Aspects of the Attorney-Client Privilege*, ABA BUS. L. TODAY (Oct. 31, 2013), *available at* https://www.americanbar.org/groups/business_law/publications/blt/2013/10/01_unger/.

13. *Id*.

14. *See, e.g.*, United States v. United Shoe Mach. Corp., 89 F. Supp. 357, 358–59 (D. Mass. 1950); *In re A*ir Crash Disaster at Sioux City, Iowa on July 19, 1989, 133 F.R.D. 515, 518 (N.D. Ill. 1990); SEC v. Beacon Hill Asset Mgmt. LLC, 231 F.R.D. 134, 138 (S.D.N.Y. 2004); Phillips v. C.R. Bard, Inc., 290 F.R.D. 615, 625 (D.Nev. 2013).

2. Common Law Confidentiality and Other Legal Protections

Generally, to assert the attorney-client privilege under the law of most common law jurisdictions, the proponent of the privilege must prove the documents or communications were "intended to be, and in fact were, kept confidential[.]"[15] Typically, this requires the proponent of the privilege to have a "reasonable expectation of confidentiality[.]"[16]

Importantly, many courts in the United States have found that the absence of a reasonable expectation of confidentiality results in a finding of no privilege. This can have a profound impact, including with respect to communications using employer-provided email.[17] In *United States ex rel. Ray v. GSD&M Idea City*, for example, the court concluded that an employee did not have "a reasonable expectation of privacy in the e-mail communications transmitted to and received from his attorney over his workplace computer using his workplace email account."[18]

---

15. United States v. Mejia, 655 F.3d 126, 132 (2d Cir. 2011). *See also* Bogle v. McClure, 332 F.3d 1347 (11th Cir. 2003).

16. *Mejia* at 133–34. *See also* Upjohn Co. v. United States, 449 U.S. 383 (1981) (allowing that the disclosure of documents to employees, even fairly low-level employees, on a need-to-know basis does not demonstrate an indifference to the confidentiality of the documents and does not waive privilege).

17. *See, e.g.*, Multiquip, Inc. v. Water Mgmt. Sys. LLC, No. CV 08-403-S-EJL-REB, 2009 WL 4261214 (D. Idaho Nov. 23, 2009) (email auto-fill function accidentally resulted in privileged documents being sent to opposing counsel, and privilege was lost); Muro v. Target Corp. 243 F.R.D. 301 (N.D. Ill. 2007) (internal emails sent to large distribution lists indicated a lack of confidentiality).

18. United States *ex rel.* Ray v. GSD&M Idea City LLC, No. 3:11-CV-1154-O, 2012 WL 12925016, at *8 (N.D. Tex. May 15, 2012). *See also* Long v. Marubeni Am. Corp., No. 05 Civ. 639 (GEL)(KNF), 2006 WL 2998671 (S.D.N.Y. Oct. 19, 2006); Aventa Learning, Inc. v. K12, Inc., 830 F. Supp. 2d 1083 (W.D. Wash. 2011).

In finding the attorney-client privilege did not apply to the emails in question, the Court observed that "[w]here . . . . . a company has explicit and straightforward guidelines addressing the monitoring of e-mail communications, an employee has no reasonable expectation of privacy in the e-mails, even if the company does not routinely enforce the monitoring policy."[19] Thus, the absence of a reasonable expectation of privacy meant the emails were unprotected by the attorney-client privilege.[20]

In this context, counsel should remain mindful of the scope of any applicable privilege in the relevant jurisdiction(s), because a failure to maintain confidentiality or to maintain the privilege in one jurisdiction can have far-ranging effects. For example, in the *RBS Rights Issue Litigation*, the English court held that English privilege law applied to communications occurring in the United States.[21] English courts tend to take a narrower view of who is the client when applying the legal-advice privilege than most U.S. courts when applying the attorney-client privilege. Thus, the *RBS* court concluded that certain information, including U.S. outside counsel's notes regarding interviews with RBS employees, was discoverable. Once information is produced, it is more vulnerable to being discoverable in other

19. *United States ex rel. Ray*, 2012 WL 12925016, at *4.

20. This rationale has been mentioned in the context of cross-border privilege issues. In *Louis Vuitton Malletier v. Dooney & Bourke, Inc.*, No. 04 CIV. 5316 RMB MHD, 2006 WL 3476735, at *16–18 (S.D.N.Y. 2006), the court analyzed a claim of privilege under U.S. law and explained that the unlicensed French attorney did not have privilege under French law. In *dicta* the court noted that the communications at issue occurred in France and stated "there is no reason to believe that there was any expectation by the participants that confidentiality could be maintained in the face of French law." *Id.* at 17. *Louis Vuitton* suggests that a company does not have a reasonable expectation of confidentiality if it places information in the hands of in-house counsel in a country that does not recognize privilege for in-house counsel.

21. *Re* RBS Rights Issue Litig. [2016] EWHC 3161 (Ch) (Eng.).

jurisdictions, because it becomes more difficult to argue that confidentiality has been maintained.

From a cross-border perspective, it also is important to keep in mind that confidentiality obligations may not be treated as a legal privilege in many jurisdictions. Many countries impose professional confidentiality obligations on attorneys, and U.S. courts have distinguished these confidentiality obligations from the attorney-client privilege.[22] If an assertion of attorney-client privilege is to be based in part on another country's professional confidentiality obligations, those obligations must be examined carefully to determine, among other things, what exceptions to the confidentiality obligations exist.

3. Common Law Definition of Attorney

Each common law jurisdiction has its own unique requirements for qualification as an attorney. For example, the United States typically defines a lawyer as a member of the bar, which commonly requires a law degree, passage of a bar examination, and proof of good ethics. Ireland requires either a law degree or a preliminary examination, an entrance examination to the Law Society of Ireland, and professional and in-office training to be admitted to the Roll of Solicitors. Northern Ireland and England and Wales follow similar requirements.

Some common and civil law jurisdictions recognize multiple categories of lawyers, and the attorney-client privilege only applies to certain categories of lawyers. Some jurisdictions, including common law jurisdictions, do not require, or may not allow, in-house counsel to be licensed attorneys, which can lead to

22. Gucci Am., Inc. v. Guess?, Inc., 271 F.R.D. 58, 67 (S.D.N.Y. 2010) (internal quotation marks and citations omitted).

inadvertent waivers of an applicable privilege.[23] In *Gucci v. Guess?*, for example, the U.S. court found that certain communications with an unlicensed patent agent in Italy were not privileged under U.S. law, because the agent's work was not supervised by an attorney, and the communications were not intended to remain confidential.[24]

4. Common Law Definition of Client

Each jurisdiction has its own unique laws and views on what constitutes a "client" for purposes of attorney-client privilege. In general, a client will be the direct beneficiary of the attorney's legal advice, which is used to further the client's interests. Having a clear understanding of who the client is and which laws may apply to a privilege determination are important considerations for a variety of issues, including which person(s) or organization(s) should maintain the possession and confidentiality of potentially privileged documents. While in most, if not all, common law jurisdictions, the attorney-client privilege and work-product doctrine apply to documents and information whether in the possession of the attorney or the client, in some civil law jurisdictions the laws protecting confidentiality and privilege apply only to information in the attorney's possession.

Further, under U.S. law, when an entity is the client, the attorney-client privilege is not automatically extended to affiliates

23. *See, e.g.*, Wultz v. Bank of China Ltd., 979 F. Supp. 2d 479 (S.D.N.Y.) (in-house counsel in China are not required to be members of the Bar, and attorney-client privilege did not apply). *But see In re* Grand Jury Subpoena Duces Tecum, 112 F.3d 910 (8th Cir. 1997) (implementing a reasonable-belief test for attorney-client privilege—if the client reasonably believe the lawyer is authorized to practice law, the attorney-client privilege will apply); Anwar v. Fairfield Greenwich Ltd., 306 F.R.D. 117 (S.D.N.Y. 2013), *aff.d*, 982 F. Supp. 2d 260 (S.D.N.Y. 2013) (despite the client's poor comprehension of Dutch law, the client knew the Dutch attorney was not licensed).

24. *Gucci*, 271 F.R.D. at 72–73.

and subsidiaries. Notably, one entity's partial ownership of another entity may not be enough to preserve the privilege if privileged information is shared between them.[25] Although the issue of whether particular jurisdictions extend the protections of the attorney-client privilege and similar doctrines to subsidiaries and affiliates is beyond the scope of this *Commentary*, different jurisdictions take various approaches to the issue, and counsel representing such corporate clients will need to understand each client's corporate structure and how that could impact privilege in relevant jurisdictions.

5. Business vs. Legal Advice

To be protected by attorney-client privilege, a communication must be for the purpose of giving or receiving legal advice. Communications that seek business advice from counsel are not entitled to the protections of the attorney-client privilege.[26] This distinction can be complex, particularly for in-house counsel who may have both legal and business functions. In-house counsel roles can vary greatly, and the advice sought from in-house counsel may or may not give rise to attorney-client privilege. It is only in circumstances where counsel's legal advice is

25. *See, e.g.*, Neuberger Berman Real Estate Income Fund, Inc. v. Lola Brown Tr. No. 1B, 230 F.R.D. 398, 416 (D. Md. 2005) (unless there is "common ownership or control" courts must engage in a "painstaking analysis to determine whether 'the third party . . . shares an identical, and not merely similar, legal interest as the client with respect to the subject matter of the communication between the client and its attorney'"); Music Sales Corp. v. Morris, No. 98CIV.9002(SAS)(FM), 1999 WL 974025 (S.D.N.Y. Oct. 26, 1999) (communications between wholly owned subsidiaries are privileged because corporations operated as a single entity).

26. *See* United States v. ChevronTexaco Corp., 241 F. Supp. 2d 1065, 1076 (N.D. Cal. 2002).

sought that the protection of privilege arises.[27] When disputes about business and legal advice in the context of privilege occur during litigation, these situations often result in painstaking analysis of what advice was being sought, by or for whom, for what purpose, and the response given.[28]

27. *See* The Sedona Conference, *Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents and Communications Generated in the Cybersecurity Context*, 21 SEDONA CONF. J. 1 (2020), 26–77, which offers legal guidance and practical guidelines regarding the application of attorney-client privilege and work-product protection in the context of cybersecurity but with some broadly applicable guidance as well. For example, communications that are about the growth of the business or profit increases even when sent to an in-house attorney would likely be considered business advice. *See, e.g.*, Fed. Trade Comm'n v. Abbvie, Inc., No. CV 14-5151, 2015 WL 8623076, at *10 (E.D. Pa. Dec. 14, 2015); *In re* Denture Cream Prods. Liab. Litig., No. 09-2051-MD, 2012 WL 5057844, at *15 (S.D. Fla. 2012) (communications about potential litigation related to product labeling were considered privileged, but marketing and business decisions about product labeling would not be privileged).

28. *See, e.g.*, Reid v. British Columbia (Egg Marketing Board), 2006 B.C.S.C. 346 (when business and legal advice are intertwined to such an extent they cannot be extricated from one another, attorney-client privilege may apply); Breneisen v. Motorola, Inc., No. 02 C 50509, 2003 WL 21530440 (N.D. Ill. July 3, 2003) (there may be a presumption that in-house counsel is giving legal advice, but this presumption is not dispositive, and in-house counsel's business advice is not protected by the attorney-client privilege); Hercules, Inc. v. Exxon Corp., 434 F. Supp. 136 (D. Del. 1977) (the attorney-client privilege applies only if the attorney is acting as a lawyer giving advice on legal implications). Note that outside counsel's provision of business advice is also not be privileged. *See, e.g.*, Koumoulis v. Indep. Fin. Mktg. Grp., Inc., 295 F.R.D. 28 (E.D.N.Y. 2013) (outside counsel's advice related to human resources during an internal investigation were not privileged).

6. Common Law Work-Product Doctrine

The work-product doctrine, known as "litigation privilege" in some jurisdictions, protects documents or information prepared or collected:[29]

1. In anticipation of litigation
2. by or for a party or its representative.

Work product can include but is not limited to communications, written statements, private memoranda, fact chronologies, mental impressions, personal beliefs, and other information assembled by attorneys or parties in anticipation of litigation, which is often broadly defined in the United States as any adversarial proceeding.[30] Work product thus is not limited to confidential communications between attorney and client, as the attorney-client privilege is. In the United States, the work-product doctrine applies to "ordinary" or fact work product (for example, materials prepared by a party in anticipation of litigation, such as fact collection and witness interviews)[31] and opinion work product (for example, an attorney's mental impressions, opinions, analysis, and conclusions). [32]

---

29. FED. R. CIV. P. 12(b)(3). *See also* Hickman v. Taylor, 329 U.S. 495 (1947); FED. R. EVID. 502(g)(2).

30. The definition of litigation is broad. *See, e.g.*, *In re* Rail Freight Fuel Surcharge Antitrust Litig., 268 F.R.D. 114, 118 (D.D.C. 2010) (protecting materials prepared for an administrative hearing); United States v. Stewart, 287 F. Supp. 2d 461, 465–67 (S.D.N.Y. 2003) (protecting materials prepared for a grand jury proceeding); Abdallah v. Coca-Cola Co., No. A1:98CV3679RWS, 2000 WL 33249254 (N.D. Ga. Jan. 25, 2000) (protecting materials prepared for a government investigation); and Jumper v. Yellow Corp., 176 F.R.D. 282 (N.D. Ill. 1997) (protecting materials prepared for arbitration).

31. *See, e.g.*, *In re* Doe, 662 F.2d 1073 (4th Cir. 1981).

32. *See, e.g.*, *In re* Vitamins Antitrust Litig., 211 F.R.D. 1 (D.D.C. 2002); Va. Elec. & Power Co. v. Sun Shipbuilding & Dry Dock Co., 68 F.R.D 397 (E.D. Va. 1975).

Though a broader set of materials could fall within the scope of the work-product doctrine, the doctrine is "weaker" than the attorney-client privilege at least with respect to fact work product in that a party could seek production of fact work product by showing need and undue hardship. Opinion work product tends to be more strongly protected, and motions to compel production of opinion work product are rarely granted. In light of how the different forms of work product are treated, counsel should carefully research how courts in the relevant jurisdiction(s) have distinguished between those categories.

Note that in some jurisdictions—such as Canada, England, and Wales—it is not necessary that the information be prepared by a lawyer or that a lawyer be involved at all for litigation privilege to apply. The question is whether the predominant purpose for the generation of the information was for use in litigation, whether existing or contemplated. A similar test applies in the majority of U.S. federal courts.

7. Common Law Waiver

As a general matter under U.S. law, the attorney-client privilege may be waived through voluntary, intentional disclosure of confidential communication to someone outside the attorney-client relationship.[33] The privilege can also be waived through inadvertent disclosure, such as by disclosing an otherwise privileged document, making a privileged document accessible to

33. *See* United States v. Kovel, 296 F.2d 918, 921–22 (2d Cir. 1961). According to the "Kovel doctrine," an agent of an attorney may be included in the privilege if the attorney supervises the agent and relies on the agent in order to be able to provide legal advice. These typically include law clerks, legal assistants, paralegals, and other employed by the attorney or the law firm but may also include outside consultants. In interpreting *Kovel*, courts have varied on whether the agent must be "necessary" to or "add value" to the attorney's work to be covered by the privilege.

someone who is not within the scope of the privilege, or by having a confidential conversation in an area where a third party can overhear it. In cases of inadvertent disclosure, the waiver determination often will turn on whether the party took reasonable steps to prevent disclosure in the first place and also acted promptly to rectify the error. Disclosure also may trigger "subject matter waiver" where "fairness requires a further disclosure of related, protected information, in order to prevent a selective and misleading presentation of evidence to the disadvantage of the adversary."[34] Subject-matter waiver is rare and typically arises only where a party tries to use the privilege as a sword and as a shield, such as by claiming he or she acted appropriately based on legal advice but then withholding disclosure of documents or information concerning the substance of that advice.[35]

Whether there has been a waiver of work product can depend on whether the work product is categorized as fact work product or opinion work product. The distinction is important because although a requesting party sometimes can overcome a work-product assertion concerning fact work product by showing substantial need (for example, disclosure of a witness interview memorandum for a witness who died), courts in the United States rarely allow discovery of legal strategies,

34. FED. R. EVID. 502 advisory committee's note. *See also In re* OM Grp. Sec. Litig., 226 F.R.D. 579 (N.D. Ohio 2005) (subject-matter waiver applied when the waiver was substantial, intentional, and deliberate).

35. *See*, *e.g.*, *In re* Grand Jury Proceedings Oct. 12, 1995, 78 F.3d 251 (6th Cir. 1996) (selective disclosure led to wider privilege waiver) and *Doe 1 v. Baylor Univ.*, 320 F.R.D. 430, 439–40 (W.D. Tex. Aug. 11, 2017) (intentional release of the law firm's factual findings and recommendations necessarily disclosed attorney-client communications and constituted sweeping privilege waiver).

counsel's opinions or mental impressions, and other opinion work product.[36]

A U.S. court's determination that another country's law applies to a privilege determination may result in a finding that the privilege or protection is inapplicable or has been waived because the other jurisdiction does not recognize the privilege or protection at all, or because the privilege or protection was waived under the particular circumstances. To assert the attorney-client privilege in the United States, it is necessary to show, among other things, that confidentiality was maintained, so an applicable privilege could be waived if the documents or information are shared with persons outside the scope of the privilege.[37] That is true even within the context of documents or information being shared among personnel within the same corporate client. For example, if the documents or information at issue were shared with in-house counsel in a jurisdiction that does not recognize privilege or other similar confidentiality or professional secrecy obligations for in-house counsel, there may be an argument that the attorney-client privilege does not apply or has been waived.[38]

8. Common Law Burden of Proof Regarding Privilege

In the United States, it is well established that the party asserting a privilege generally has the burden of proof.[39] This

36. *See* United Coal Cos. v. Powell Constr. Co., 839 F.2d 958 (3d Cir. 1988).

37. *See* United States v. Mejia, 655 F.3d 126, 132 (2d Cir. 2011).

38. *See, e.g.*, Louis Vuitton Malletier v. Dooney & Bourke, Inc., No. 04-CV-5316-RMB-MHD, 2006 WL 3476735 (S.D.N.Y. Nov. 30, 2006); Shire Development, Inc. v. Cadila Healthcare Ltd., No. 10-581-KAJ, 2012 WL 5331564 (D. Del. Oct. 19, 2012); and Veleron Holding, B.V., v. BNP Paribas SA, No. 12-CV-5966-CM-RLE, 2014 WL 4184806 (S.D.N.Y. Aug. 22, 2014).

39. *See, e.g.*, United States v. Jones, 696 F.2d 1069 (4th Cir. 1982); Weil v. Inv./Indicators, Research and Mgmt., Inc., 647 F.2d 18 (9th Cir. 1981). *But see*

means that the party generally has the burden to establish that a privilege should be recognized under the relevant law. If a party asserting the privilege argues that documents should be protected because they would be privileged in another country, then that party also has the burden of demonstrating that the other country's law should be applied.

9. Common Law Choice of Law

Choice-of-law analysis, discussed in additional detail in Sections III.H and IV, determines which laws a court in one country will apply to decide whether a privilege may be validly asserted.[40] For example, in the United States, a court may choose to apply the laws of another country using accepted forms of analyses. However, even when U.S. courts (and even courts within the same judicial district) purport to apply the same choice-of-law analyses, they have reached different outcomes in similar scenarios. For example, federal courts in the Second Circuit use the "touch base" test to determine which country's privilege laws apply. In *Wultz v. Bank of China Ltd.*, the court described the "touch base" test as follows:

> Under this analysis, the Court applies the law of the country that has the predominant or the most direct and compelling interest in whether [the] communications should remain confidential, unless that foreign law is contrary to the public policy of this forum. The country with the predominant interest is either the place where the allegedly privileged relationship was entered into or the place in which that relationship was

Sampson v. Sch. Dist. of Lancaster, 262 F.R.D. 469 (E.D. Pa. 2008); Texaco, Inc. v. La. Land & Exploration Co., 805 F. Supp. 385 (M.D. La. 1992).

40. *See* FED. R. CIV. P. 44.1; FED. R. EVID. 501; RESTATEMENT (SECOND) OF CONFLICT OF LAWS (AM. LAW INST. 1971); Hague Convention art. 11.

> centered at the time the communication was sent. Thus, American law typically applies to communications concerning legal proceedings in the United States or advice regarding American law, while communications relating to foreign legal proceeding[s] or foreign law are generally governed by foreign privilege law.[41]

In *Wultz*, Judge Shira Scheindlin of the Southern District of New York determined that U.S. privilege law would apply to all communications related to U.S. legal issues.[42] However, applying this same "touch base" test, Judge Barbara Jones of the Southern District of New York reached a notably different result[43] in *Astra Aktiebolag v. Andrx Pharmaceuticals, Inc.*, deciding that U.S. privilege law would apply to all communications.[44]

Additionally, in some jurisdictions, determining which law applies can turn on whether the privilege is considered a matter of procedure or a substantive rule of law. For example, when an action brought in a Canadian court involves claims governed by laws of another jurisdiction, the general rule is that matters of procedure continue to be governed by the laws of the forum.[45]

---

41. Wultz v. Bank of China Ltd., 979 F. Supp. 2d 479, 486 (S.D.N.Y. 2013) *on reconsideration in part*, 11 CIV. 1266 SAS, 2013 WL 6098484 (S.D.N.Y. Nov. 20, 2013) (internal quotation marks and footnotes omitted).

42. *Id.* at 492, *modified on reconsideration*, 2013 WL 6098484, at *2 (Nov. 20, 2013) (clarifying the scope of the privilege).

43. *See* Teradata Corp. v. SAP SE, U.S. Dist. LEXIS 232053 *43–47 (N.D. Cal. Sept. 9, 2019) for a further analysis of the different results reached by Judge Jones.

44. Astra Aktiebolag v. Andrx Pharm. Inc., 208 F.R.D. 92, 101–02 (S.D.N.Y. 2002). The decision protected Korean documents that would have been deemed nonprivileged under Korean law (although nondiscoverable under Korean discovery rules).

45. Livesley v. Horst Co., [1924] S.C.R. 605, 608 (Can.).

Traditionally, Anglo-Canadian courts have classified solicitor-client privilege as a matter of procedure rather than as a substantive rule of law. As a result, the question of whether a person can claim the privilege in a legal proceeding is a matter of procedure to be determined by the law of the forum.[46]

This position is further illustrated in *Lawrence v. Campbell*, the seminal English case on cross-border privilege.[47] The issue in *Lawrence* was whether the communications between Scottish lawyers practicing Scottish law in England and their Scottish client in Scotland were privileged. A plaintiff brought an action in England against both the Scottish client and the Scottish lawyer. English law recognized the privilege and would have prevented documentary production, though this arguably would not have been the outcome under Scottish law. The Court held that the communications were privileged since the governing law was that of England rather than Scotland. Vice Chancellor Sir Richard Kindersley stated:

> A question has been raised as to whether the privilege in the present case is an English or a Scotch privilege; but sitting in an English Court, I can only apply the English rule as to privilege, and I think that the English rule as to privilege applies to a Scotch solicitor and law agent practising in London, and therefore the letters in question are privileged from production.[48]

Lawrence was followed by *Re Duncan*, which dealt with communications between an English client and a non-English

46. *See* Oilworld Supply Co v. Audas, [1985] B.C.J. No. 1472 (Can.), where Judge William Campbell stated "it is well established that questions as to . . . privilege are matters of procedure governed by the law of the *lex fori*."

47. Lawrence v. Campbell [1859] 62 Eng. Rep. 186.

48. *Id.* at 491.

lawyer.[49] The plaintiff, who was challenging a foreign will, had consulted with a lawyer outside of England before eventually bringing the proceeding in an English court. The defendant argued that the communications should be disclosed on the basis that no privilege was recognized in the other jurisdiction. Lord Justice Ormrod found this argument inconsistent with *Lawrence* and held that the law of the forum governs solicitor-client privilege. As a result, the plaintiff was entitled to assert solicitor-client privilege over communications with his non-English lawyer. *Re Duncan* has also been followed in Canada.[50]

B. Civil Law Privilege and Other Legal Protections

1. Origin of Civil Law Privilege

In civil law countries, judges are central to determining the type of evidence needed for a matter and generally closely control the disclosure process. Because of the limited discovery in civil law countries, there has been less need to build out the complex privilege protections regularly found in common law jurisdictions. Statutes further govern the legal profession by way of civil law professional confidentiality or secrecy obligations. This means that instead of traditional "attorney-client privilege" as understood in many common law countries, civil law protects the confidentiality of communications between attorneys and their clients through "legal professional privilege."

---

49. *Re* Duncan, [1968] 2 W.L.R. 1479 (Can.).

50. *See, e.g.*, Morrison-Knudsen Co. v. British Columbia Hydro & Power Auth., [1971] 3 W.W.R. 71 (Can. B.C.S.C.). Citing *Re Duncan* for the premise that advice from a foreign lawyer can fall within the scope of the solicitor-client privilege. The communications in question were between American in-house counsel of an American parent company and officers of that company's Canadian subsidiary. The court held that those communications were privileged on the basis that the communications would have been privileged had they occurred in Canada.

Notably, in many civil law jurisdictions, an in-house lawyer by definition cannot qualify as an attorney, meaning no attorney-client privilege can extend to in-house counsel. Thus, in some jurisdictions, information in the hands of in-house counsel may have no protection, and providing them with access to otherwise privileged materials may waive the privilege. Whether a particular document is protected may turn on whether it was created by outside counsel, how it was shared with in-house counsel, and where it is stored (i.e., who has possession, custody, or control of the document).

2. Types of Civil Law Privilege

The civil law legal professional privilege belongs to the lawyer rather than the client, and this privilege cannot be waived. Because the legal professional privilege and professional secrecy are obligations of the lawyer, a client cannot authorize a lawyer to divulge the privileged information to a third party, as can typically be done in common law jurisdictions. A number of civil law countries, including Belgium, France, Germany, and Italy, impose criminal sanctions on lawyers who violate legal professional privilege.

Litigation privilege, which is similar to the common law work-product protection discussed above, may exist in civil law jurisdictions, but the protections afforded by the litigation privilege are typically more limited and vary significantly by jurisdiction.

3. Civil Law Duty of Confidentiality

Many civil law jurisdictions recognize that attorneys, working in their capacity as attorneys, have a duty not to disclose confidential communications of their clients. Civil law jurisdictions do not generally consider this a privilege but a duty of confidentiality or professional secrecy. Clients may not be able to

waive this duty of attorneys, but clients may themselves choose to disclose the confidential information.

While most civil law jurisdictions recognize the special relationship between attorney and client in some form, the scope of protection the relationship affords can differ greatly.[51] In many civil law jurisdictions, the risk of disclosure is minimal, as parties simply disclose to other parties only what they wish to disclose.[52] Thus, communications themselves are not privileged, but lawyers have a duty not to disclose the information contained within the communications. Most civil law jurisdictions also do not have a formal process of disclosure, but the parties may apply for a court order that the opposing party or a third party disclose one or more specific, clearly defined documents containing relevant evidence of important facts. Many civil law jurisdictions provide attorneys the opportunity to resist such production orders through proof of a confidentiality obligation or other extenuating circumstances.

As the world becomes increasingly interconnected, companies involved in multinational business operations require extensive communications with their attorneys. A company is at risk of being involved in litigation in jurisdictions where they do business and may thus be subject to the laws of the forum country in determining the scope of privilege. Inconsistent rules applying to multinational communications bring greater risks to lawyers and clients alike, especially in maintaining

---

51. Steven C. Bennett, *International Issues in Privilege Protection: Practical Solutions*, 82 U.S. L. WEEK 708 (2013), *available at* https://www.jonesday.com/files/Publication/123b31e2-e3a2-4849-ba42-7d61bd10db3e/Presentation/PublicationAttachment/dd0de71e-159b-4860-9b69-ed53d12c787c/bennettprivilege%20protection.pdf.

52. Philip M. Berkowitz, *The Attorney-Client Privilege and Advising Across Borders*, LITTLER MENDELSON (Nov. 29, 2013), https://www.littler.com/publication-press/press/attorney-client-privilege-and-advising-across-borders.

privilege.[53] For example, the European Union (EU) has drawn a clear distinction between communication with lawyers designated as *in-house counsel* and *outside counsel* in determining whether the communication is privileged, where communications between in-house counsel and others at the corporation are not considered privileged.[54]

4. Civil Law Choice of Law

Many civil law jurisdictions, including, for example, Germany and Switzerland, have no specific choice-of-law rules governing privilege. These civil law jurisdictions may determine that a third-country's privilege laws apply in some circumstances, such as when evidence is obtained through a request for mutual legal assistance in another country.[55] However, it should not generally be expected that the privilege applicable in common law jurisdictions will be applicable in civil law jurisdictions. For example, French courts have held that discovery compelled in France is subject to French law even if the compelled materials contained U.S. documents (and despite the French court's ability to determine the merits of the matter through the application of U.S. law if it wished).[56] French courts will, however, apply another country's privilege laws to information exchanged or relationships established entirely outside

53. Nina Macpherson & Theodore III Stevenson, *Attorney-Client Privilege in an Interconnected World*, 29 ANTITRUST 28 (2015).

54. Akzo Nobel Chems. Ltd. v. Comm'n of the European Cmtys., 2008 Bus. L.R. 348 (Ct. of First Instance 2007).

55. *See* Bundesgerichtshof [BGH] [Federal Court of Justice] Nov. 21, 2012, 1 Strafsenats [StR] 310/12 (Ger.), noting that there is a broad consensus that prohibitions on the use of evidence obtained through mutual legal assistance could arise due to either the domestic legal system of the requesting state or the principles of international law.

56. French Supreme Court, 1st Civil Section, Nov. 3, 2016, 15-20495; French Supreme Court, 1st Civil Section, July 4, 2007, 04-15.367.

of France. Other civil law countries, such as Brazil and the United Arab Emirates, will not typically apply another country's law if it conflicts with their own rules related to attorney-client privilege.

III. PRACTICE POINTS FOR ADDRESSING CROSS-BORDER PRIVILEGE ISSUES

A. Practice Point 1: Remain Mindful That Approaches to Privilege Differ

The substantial differences between, and even within, civil law and common law jurisdictions mean that counsel, courts, and parties must identify what potential privileges and protections are available, and what waiver risks there are, under the law of each jurisdiction as early as possible. In-house and outside counsel working regularly in particular jurisdictions should be knowledgeable regarding the common privilege distinctions they will encounter, so that they can take proactive steps to protect documents and information.

Protections afforded to documents and information related to a party's communications with counsel and attorney work-product protections vary by jurisdiction. Identical materials may be privileged in one jurisdiction but not another. For example, in the *RBS Rights Issue Litigation*, the English court held that English privilege law applied because the litigation forum was England, even though the legal advice was provided in the United States.[57] English courts take a narrower view of who the client is when applying the legal-advice privilege than most U.S. courts do when applying the attorney-client privilege.[58] Thus, the *RBS* court concluded that some information, including U.S. outside counsel's notes and other materials regarding interviews with RBS employees, were not privileged and were discoverable in England. Once information is produced in one jurisdiction, there is a greater likelihood that it will be discoverable in other jurisdictions. Thus, in establishing and

57. RBS Rights Issue Litig. [2016] EWHC 3161 (Ch).

58. *Id*.

maintaining privilege, care must be taken to anticipate where the otherwise privileged information might be relevant and requested and what steps can be taken to mitigate risk.

If a jurisdiction does not recognize a "privilege," the jurisdiction may afford other disclosure protections such as under a theory of confidentiality. Many countries impose confidentiality obligations on attorneys. However, some U.S. courts have distinguished confidentiality obligations from the attorney-client privilege:

> [A] professional secrecy obligation is not an evidentiary privilege—a critical distinction . . . . [S]imply because a [foreign] statute requires a party to keep clients' affairs secret does not mean that a privilege exists. A foreign tribunal may compel disclosure if it determines the need for the information is sufficient to outweigh the secrecy obligation, while the privilege, in contrast, is absolute and inviolate.[59]

If a party grounds a privilege assertion in another country's confidentiality obligations, the party must carefully examine those obligations to determine, among other things, whether exceptions to the confidentiality exist. For example, confidentiality obligations in civil law jurisdictions often do not cover documents possessed by a client, which may support waiver in common law jurisdictions where confidentiality is a required component of the attorney-client privilege.

Work-product protection generally is only available in common law jurisdictions. Many civil law jurisdictions either limit or do not recognize similar work-product protections. Attorneys should take precautions when creating documents in

59. Gucci Am., Inc. v. Guess?, Inc., 271 F.R.D. 58, 67 (internal quotation marks and citations omitted).

anticipation of litigation and in determining whether and to whom to disclose their work product in the context of multi-jurisdictional matters. Such precautions include determining whether in-person meetings and conference calls can substitute at times for written, and therefore more readily discoverable, communications.

B. Practice Point 2: Be Aware of the Limitations on In-House Counsel Privilege

The application of disclosure protection laws can vary depending on whether in-house counsel or outside counsel created or participated in the putatively protected documents.[60] The differences in these attorney roles have implications for privilege and other disclosure protections in the jurisdictions that recognize them. For outside counsel, privilege is clearly defined by the attorney-client relationship, although there are jurisdictional nuances regarding who within an entity can be deemed the client for the purposes of the privilege.[61] Similarly, interactions between in-house counsel and their outside counsel are well established within the attorney-client relationship and are generally privileged or protected, but there are many

60. *See also* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery and Data Protection*, 17 SEDONA CONF. J. 397 (2016) (providing more detailed guidance for in-house counsel navigating cross-border data transfer and discovery issues).

61. For example, in the United States, employees generally have been recognized as being able to have privileged communications with in-house counsel regardless of the level of their position in the company. *See* Upjohn Co. v. United States, 449 U.S. 383, 390 (1981). England uses a more limited definition of the client. *See* Three Rivers District Council v. Governor and Company of the Bank of England (No. 5) [2003] EWCA (Civ) 474 (Eng.) (holding that only those employees with express or implicit authority to seek and receive legal advice on behalf of the company could qualify as the client for purposes of privilege).

jurisdictional variants as to whether in-house counsel may be considered an attorney to the client company employing the in-house counsel. Communications between in-house counsel and their outside nonlegal, third-party contractors (such as public relations firms, experts, eDiscovery vendors, and accountants) are less clearly defined. For example, under English law, such communications would not be privileged, although they may be under U.S. law.[62]

Within many organizations, in-house counsel plays a dual role as legal adviser and as business adviser. Context can affect whether privilege attaches to those communications and advice in different jurisdictions, because privilege typically only attaches to those instances when the in-house counsel is acting as a legal adviser.[63] In-house counsel should be mindful of these

---

62. *See, e.g.*, *Three Rivers District Council* (communications with third parties could not be considered protected by the attorney-client privilege); Pricewaterhouse Coopers v. Commr of Taxation of the Commonwealth of Australia [2004] FCAFC 122 (finding there was no reason to prevent privilege from being claimed for third-party communications, as legal counsel frequently relied on outside assistance to give accurate legal advice given the complexities of modern business); *In re* Bieter Co., 16 F.3d 929 (8th Cir. 1994) (if a nonemployee contractor is the functional equivalent of an employee, privilege can attach). Note courts differ widely on this in the United States, and expert advice is encouraged if the work of third-party contractors is being completed under attorney-client privilege.

63. *See, e.g.*, U.S. Postal Serv. v. Phelps Dodge Refining Corp., 852 F.Supp. 156 (E.D.N.Y. 1994). Courts have also varied as to what is a legal and business function for in-house counsel. For example, some courts have determined that in-house counsel participating in a negotiation is functioning in a business role. Georgia Pacific v. GAF Roofing Mfg. Corp., 1996 WL 29392 (S.D.N.Y. Jan. 25, 1996). *See also* MSF Holdings, Ltd. v. Fiduciary Trust Co., Int'l, 2005 WL 3338510 (S.D.N.Y. Dec. 7, 2005) (in-house counsels' communications did not include specific references to legal principles or contain legal analysis, so the communications were deemed to be of a predominantly business nature and not privileged).

issues and consider clearly separating communications into business advice and legal advice whenever possible.[64]

For in-house counsel, the "client" is generally considered to be the legal entity employing the in-house counsel; however, certain jurisdictions define the client more narrowly. Many civil law jurisdictions find that in-house counsel is not sufficiently independent to provide legal advice to the corporate client, so privilege cannot attach to in-house counsel work.[65] Therefore, when in-house counsel communicates with other employees, or former employees, those communications may not be privileged. This is also the case in some common law jurisdictions, which may only recognize a limited in-house counsel privilege. For example, in the English *Glaxo Wellcome* case, emails between an in-house counsel and an employee gathering information to provide to external lawyers were not protected by the legal-

64. One admittedly time-intensive example of how this could be done is through a "charging memo," which is documentation provided to a specific set of people, laying out the scope of work, explaining the legal reasons for the work, and providing instructions on the steps and appropriate privilege or confidentiality labeling that employees should take. Recipients should then acknowledge this document and records maintained. In-house counsel would also need to update the memo regularly as the scope of work or instructions change. Additionally, in-house counsel can consider providing training for employees on handling and protecting privilege, both in general and on a project-specific basis, including communication planning, data storage, and standard labeling conventions.

65. A notable exception is Spain, which recently passed a law explicitly laying out that in-house counsel will be subject to a separate lawyers labor agreement that recognizes the independence and legal privilege required to practice in the legal profession. *See Real Decreto 135/2021, de 2 de marzo, por el que se aprueba el Estatuto General de la Abogacía Española* (March 24, 2021), *available at* https://www.boe.es/boe/dias/2021/03/24/pdfs/BOE-A-2021-4568.pdf; Marten Männis, *A Giant Leap Forward in Continental Europe Toward Full Unification of the Legal Profession—legal privilege for Spanish in-house lawyers clarified and enshrined in law*, IN-HOUSE LEGAL (March 8, 2021), *available at* https://inhouse-legal.eu/legal-privilege/spanish-decree-law/.

advice privilege.[66] Similarly, England's *Three Rivers* case found that internal communications, even with the intent of sharing the information with outside counsel, were not privileged.[67] With respect to in-house counsel, the extent to which any privilege applies can also vary depending on the specific function, licensing, or certification of the in-house counsel.[68]

Particularly at the outset of litigation, in-house counsel should be mindful of potential challenges to privilege and aware that engaging outside counsel to provide legal advice may help to protect privilege in some situations.[69] In-house counsel responsible for contract negotiations should coordinate with litigation counsel (in-house or outside) to ensure that contractual choice-of-law clauses make sense for the entity, as these

66. Glaxo Wellcome UK Ltd (t/a Allen & Hanburys) & anr v Sandoz Ltd & ors [2018] EWHC 2747 (Ch) (Eng.). In *WH Holding Ltd v E20 Stadium LLP* [2018] EWCA Civ 2652 (Eng.), the England & Wales Court of Appeal held that emails between board members, which had been prepared for the purpose of discussing a settlement proposal of a dispute, were not covered by litigation privilege. The court held that litigation privilege is restricted to circumstances where the dominant purpose of communications is for obtaining advice or information, not the conduct of litigation more broadly.

67. *Three Rivers District Council,* [2003] EWCA (Civ) 474 (Eng.) Note that this decision has been divisive, and the Hong Kong Court of Appeals found the decision unworkable, deciding instead that the appropriate test for determining privilege within an entity was the "dominant purpose" test. Citic Pacific v. Secretary of Justice [2012] 2 H.K.L.R.D. 701.

68. *See* Sundenga Indus., Inc. v. Global Indus., Inc., No. 18-2498-DDC, 2020 WL 2513072 at *5 (May 15, 2020 D. Kan.) (noting that U.S. judges have "distinguished between countries where in-house counsel are not required to be members of the bar or have some form of legal credentials, such as China or the Netherlands, and those where they are" when determining the applicability of the attorney-client privilege).

69. Note that the engagement of outside counsel must involve legal advice. The engagement of outside counsel merely as a means to maintain the color of privilege would not likely be effective and would be unlikely to gain favor with courts or opposing parties.

can have serious impacts on privilege if litigation or arbitration arises later. Actions taken at an early stage of a matter without due consideration of the privilege implications may have later consequences that cannot be remedied. Furthermore, these consequences may crystallize in jurisdictions that are not contemplated at those early stages. Take, for example, an investigation by the European Commission. Under EU antitrust case law, the attorney-client privilege does not protect documents prepared by in-house lawyers or the in-house lawyer's communications with company colleagues. Disclosure of in-house work product to the European Commission may prompt later arguments that the disclosure amounted to a waiver of privilege elsewhere.

Figure 1 (below) shows a decision tree that in-house counsel based in Europe could follow in assessing whether a privilege will cover documents and other information and whether, for example, U.S. privilege law may apply. The first step in the assessment is understanding who wants or will want the document or information. For example, if the inquiry is being made by a national regulator, much will depend on which authority is seeking the documents or information, and thus the specific laws that may apply. Similarly, if the documents or information are being sought by, or are likely to be sought by, a private party, in-house counsel should examine which jurisdictions' laws could apply. If there is an action in the United States, for example, and there is an argument that the communications "touch base" with the United States or the United States has the most significant interest in the communication, then U.S. privilege law may apply. In that scenario, if other conditions for the privilege to apply are satisfied (i.e., the communication was confidential, between attorney and client, and for the purpose of giving or receiving legal advice), the communication is more likely to be protected.

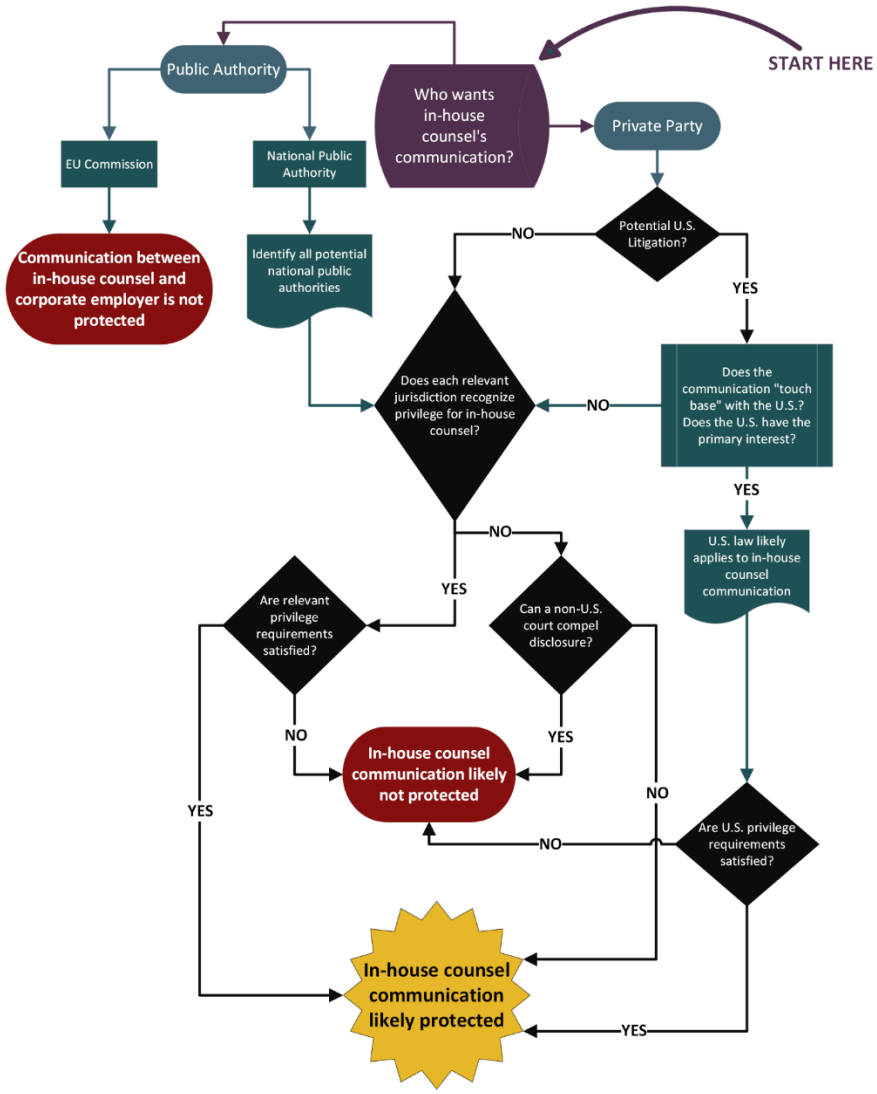


Figure 1. An example of the analysis EU in-house counsel might take to understand applicable privileges.

C. *Practice Point 3: Consider Applicable Governmental and Regulatory Privileges and Weigh the Risks of Waiver before Making a Regulatory Disclosure*

Counsel should consider whether documents are subject to regulatory privileges, such as confidential supervisory information or the bank-examiner privilege, which are held by regulators. Supervisory regulatory privileges vary greatly by jurisdiction and can affect the disclosure of documents, such as when voluntary disclosure is desired by a client but refused by a regulator holding the privilege.

Additionally, before disclosing materials to a regulatory body, counsel must consider what effect such disclosure may have on their clients' interests in other jurisdictions. Disclosures in one jurisdiction may contribute to a finding that privilege has been waived in another. The confidentiality of such document disclosures also may not be guaranteed. For example, governments may share documents with other governments through requests or information sharing agreements. While some regulatory bodies treat all disclosures as confidential (and thus an argument can be made that privilege has not been waived), others do not, and disclosure in that jurisdiction may be considered waiver in another. For example, in Canada, a disclosure of documents to the Competition Bureau under a Section 11 Order for the production of documents is considered "confidential."[70] That is, the Canadian Competition Bureau will not further disclose any of the documents provided under the Order.

In the United States, by contrast, disclosure to a governmental agency is more likely to result in a waiver of applicable privileges or protections. For example, the U.S. Court of Appeals for the Ninth Circuit held that if a party provides attorney-client privileged materials to the government, the party cannot later

70. Competition Act, R.S.C. 1985, §§10(3) and 29.

claim privilege over the same materials in civil litigation.[71] In another recent Ninth Circuit case dealing with whistleblower retaliation, *Wadler v. Bio-Rad*, the court found that not only had Bio-Rad previously waived any applicable privileges by disclosing relevant communications to the governmental agencies in pre-suit investigations and administrative proceedings, but that Wadler could rely on the privileged communications necessary to prove his case.[72]

Counsel must work with their clients to consider generally the upside of government or regulatory cooperation with the potential downside of the loss of privilege or other protections. Counsel should also consider when and how to reasonably limit the production of documents and information to governments and regulators through, for example, trying to negotiate a narrower scope for requests and the redaction of protected information.

---

71. *In re* Pac. Pictures Corp., No. 11-71844, 2012 WL 1293534 (9th Cir. Apr. 17, 2012). The Eighth Circuit, in contrast, recognizes limited or selective waiver, in which voluntary disclosure to the government, which is often done in order to cooperate with an investigation, does not waive the privilege. Diversified Industries, Inc. v. Meredith, 572 F.2d 596 (8th Cir. 1977) (en banc). All other U.S. circuit courts have rejected the limited waiver of *Diversified Industries.*

72. Wadler v. Bio-Rad Laboratories, Inc., No. 15-cv-023560-JCS, 2016 WL 7369246 (N.D. Cal. Dec. 20, 2016). Further, the Court recognized Rule 1.6 of the Model Rules of Professional Conduct, which permits an attorney to reveal privileged information when that information is required to establish a claim or defense related to "a controversy between the lawyer and the client." Privilege is an important factor to encourage whistleblowing. Both compliance and law enforcement consider this to be critical, especially as many major international fraud investigations have begun with a whistleblower who might not have come forward absent such protections.

D. Practice Point 4: Be Proactive in Exploring and Exercising Options to Protect Applicable Privileges

Counsel should be diligent in exercising all available options in protecting the privilege and other disclosure protections at all stages of a representation.[73] Counsel, both in-house and outside, should consider privilege issues early and regularly as part of both general litigation preparedness and specific matter planning, identifying how to protect documents under relevant different privileges and different privilege regimes. Counsel should consider which jurisdictions might have an interest in a client or a specific matter. It is often prudent to assume that the least protective privilege law may apply. Counsel should not assume that broad U.S. privilege protections will apply in other countries.[74]

Counsel should also consider and utilize properly drafted confidentiality agreements and protective orders, which can provide limited protections to privileged materials disclosed in litigation.[75] U.S. courts may order both confidentiality

---

73. For additional guidance on protecting electronically stored information (ESI), *see* The Sedona Conference, *Commentary on Protection of Privileged ESI*, 17 SEDONA CONF. J. 95 (2016). This publication also has valuable guidance on the implementation of protective orders to safeguard privilege in U.S. litigation.

74. *See* RBS Rights Issue Litig. [2016] EWHC 3161 (Ch) (Eng.).

75. *See, e.g.*, Tenneco Packaging Specialty & Consumer Prods., Inc. v. S.C. Johnson & Son, Inc., No. 98 C 2679, 1999 WL 754748 (N.D. Ill. Sept. 14, 1999) (confidentiality agreement helped to preserve privilege in a dispute about waiver). *See also* The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition),* Appendix C: Model U.S. Federal Court Protective Order (January 2017), *available at* https://thesedonaconference.org/publication/International_Litigation_Principles [hereinafter *Sedona Conference International Litigation Principles*], which includes a "No Waiver of Privilege Provision" and other privilege protections. Principle 4 of The Sedona Conference International Principles also

agreements that include nonwaiver provisions and protective orders that can be binding in other U.S. litigation.[76] However, these will not necessarily provide protection in non-U.S. jurisdictions or during governmental or regulatory investigations. A court-sanctioned protective order can be implemented to include provisions in which both sides agree that inadvertent disclosure does not constitute waiver (i.e., that such disclosure remains confidential), and that the material cannot be used in any other proceeding. Absent specific agreement between the parties, protective orders may not govern the use of inadvertently produced privileged materials, and inadvertent disclosures in U.S. litigation can still lead to privilege disputes between the parties. Similar agreements are regularly utilized as part of document exchange protocols in Canada.

Because many jurisdictions do not recognize in-house counsel privileges or protections, knowing when to engage and leverage the expertise of outside counsel is advised. Even in common law jurisdictions, judicious engagement of outside counsel may help to avoid the complex legal-versus-business advice analysis that often occurs in privilege disputes about in-house counsel functions, as the engagement of outside counsel to provide legal advice offers a clearer delineation between legal and business functions. In multijurisdictional matters, consider whether engaging local counsel from the relevant jurisdiction(s) with the broadest privilege or disclosure protections would be helpful. When it is contemplated or likely that an engagement will involve activities in more than one jurisdiction, the attorney

supports the use of protective orders in the context of minimizing conflicts between data protection laws and U.S. discovery demands.

76. *See* FED. R. EVID. 502, which limits subject-matter waiver and allows additional protections through protective orders (often called 502(d) orders in U.S. litigation). *See also* Rajala v. McGuire Woods, LLP, No. 08-2638-CM-DJW, 2013 WL 50200 (D. Kan. Jan 3, 2013).

being engaged should be able to advise the client on the potential risks associated with varying and conflicting laws concerning privilege. Using local counsel in another country to assist in navigating that jurisdiction's privilege framework can provide critical guidance and value. Further, retaining local counsel in other jurisdictions may, depending on the jurisdiction, support the protection of privilege under the other jurisdiction's rules.

Privilege is not only a litigation issue. Counsel must consider the nature of a particular client engagement as well, such as whether the engagement is for advice related to a commercial matter where there is no litigation, or for assistance on an adversarial matter related to a dispute. Nonlitigation advice related to privilege may require assistance with issues, such as choice-of-law clauses, to help proactively protect privilege.[77] For engagements related to disputes, counsel will need to help best negotiate maintaining the privilege and marshal the most compelling arguments for the strongest privilege to apply. However, counsel may have little input or ability to determine retroactively which jurisdiction's privileges will apply. Some courts, for example, equate anticipation of litigation for triggering the preservation obligation with anticipation of litigation for purposes of identifying protectable work product.[78] Where that is

77. *See also* The Sedona Conference, *Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders*, 21 SEDONA CONF. J. 393, 423 (2020). "In commercial transactions in which the con-tracting parties have comparable bargaining power, the informed choice of the parties to a contract should determine the jurisdiction or applicable law with respect to the processing of personal data in connection with the respective commercial transaction, and such choice should be respected so long as it bears a reasonable nexus to the parties and the transaction." This advice can reasonably be extended to matters of privilege as well.

78. *See, e.g.*, LendingTree, LLC v. Zillow, Inc., No. 3:10-CV-00439, 2014 WL 1309305, at *10 (W.D.N.C. March 31, 2014) ("duty to preserve evidence arose no later than its assertion of the attorney work product privilege"); Siani v.

the case, timely legal holds may also help to define the scope of work-product protections by indicating a starting date for the work-product protection to apply.[79] However, for clarity, legal holds themselves do not confer any privilege status on the documents and information under legal hold.

Counsel are responsible for informing their clients about privilege—when it exists, how to protect it, and when it can be waived—so that clients can make informed choices. For example, in common law jurisdictions, it is important for clients to understand that privilege belongs to the client, not the counsel. Clients need to understand that as it is their privilege, they are able to waive it, inadvertently or otherwise. Clients should be informed that all documents and discussions related to a litigation must remain private and confidential (must not be communicated to third parties) or the privilege is lost. When working with corporate clients, counsel should ensure that work performed by nonlawyers, including third parties, is appropriately labeled and identified as privileged or protected when appropriate. In-house counsel may need to offer specific training to help others in the organization understand when they are working on privileged projects and how to stamp or brand related documents to help preserve privilege. Although the identification of documents as privileged is not dispositive, a protocol for such work will be invaluable in assisting outside counsel with understanding when particular stamping or branding is implemented in order to best protect client documents.

State Univ. of N.Y. at Farmingdale, No. CV09-407 (JFB)(WDW), 2010 WL 3170664 (E.D.N.Y. Aug. 10, 2010) (if litigation foreseeable for work product, it was reasonably foreseeable to trigger preservation).

79. For additional information on legal holds, see The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341 (2019).

Counsel should be mindful of and inform their clients about data residency concerns. While clients and counsel may believe that documents they author are stored locally on their laptop or on a server in their office, this setup is often not the case. Many large corporations and law firms have moved to cloud-based storage, which may or may not be storing the data in the jurisdiction where it is created. Furthermore, the use of certain publicly available services, such as Google Translate or Apple's virtual assistant, Siri, may void the privilege and may violate professional secrecy obligations in many jurisdictions. These services may additionally route information to other jurisdictions or potentially affect the confidentiality of the information. Similar to other issues regarding the transmission of privileged materials to another jurisdiction, storing data in a certain jurisdiction but accessing it from another can raise concerns about confidentiality and privilege, especially in instances where individuals in (or outside) the storage jurisdiction have access to that privileged content. However, certain issues may be mitigated through, for example, access controls and the use of a formal vendor engagement program that assesses vendor risk and imposes strict confidentiality obligations on vendors.

When traveling, it is important for counsel to understand that invasive searches of electronic devices could open up the entirety of the data in the attorney's (or client's) possession to border investigators.[80] For example, if border agents search a device that is connected to a cloud server, then they may have access to all files to which the individual has access. Individuals with access to privileged content on their devices or access to cloud servers should take care to limit the privileged content

80. *See, e.g.*, U.S. v Kim, 103 F. Supp. 3d 32 (D.D.C. 2015); *see also* Riley v. California, 573 U.S. 373 (2014).

they are carrying and disconnect from those servers before crossing any border to maintain the confidentiality of data.[81]

Proactive planning should also include consideration of the other protections that could apply to protect documents from disclosure when privilege may not. For example, professional duties of confidentiality, secrecy laws and other obligations, blocking statutes, and even data protection laws. Data protection laws, such as the EU's General Data Protection Regulation,[82] prevent the disclosure of personal data without a valid legal basis and concomitant protections of that data during and after transfer. Although not intended as laws to protect legal privileges, data protection laws and related privacy safeguards typically contain strict confidentiality obligations and disclosure restrictions that may, when applicable, provide supplementary grounds for refusing to disclose privileged or other protected information that contains personal data.

E. Practice Point 5: Assess Possible Privilege Waivers and Take Practical Steps to Minimize Waiver Risks Going Forward

Counsel should assess whether there has been a waiver of an applicable privilege by determining who has had access to the

---

81. Rawles, Lee, *Traveling lawyer get new protections in device searches at border*, ABAJOURNAL (Jan. 25, 2018), https://www.abajournal.com/news/article/new_guidelines_for_electronic_device_searches_at_us_borders_will_impact_att; American Bar Association Center for Professional Responsibility, Electronic Device Advisory for Mid-Year Meeting Attendees (2018), *available at* https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/scepr_electronic_device_advisory_exec_summary.pdf.

82. 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 (General Data Protection Regulation), 2016 O.J. (L119/1) *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents.EU 2016/679.

documents or information, whether there was a prior disclosure to any third parties, identifying to whom disclosure was made, and understanding the circumstances of that disclosure. With respect to documents and information subject to disclosure, counsel should set up a defensible privilege review protocol and act immediately to retrieve any inadvertently disclosed privileged documents or information.

A U.S. court's determination that another country's law applies to a privilege determination can result in a finding that a protection is inapplicable or was waived because the other jurisdiction does not recognize the protection at all, or because the protection was waived under the particular circumstances. For example, to receive the protection of the attorney-client privilege in the United States, it is necessary to show, among other things, that the communication was kept confidential.[83] And, even if confidentiality was maintained within a corporate party, the privilege may be waived if the communication was shared with someone to whom the privilege does not apply. For example, if a communication is made accessible to in-house counsel in a jurisdiction that does not recognize the privilege for in-house counsel, a court could find the attorney-client privilege has been waived based on the rationale that the information was disclosed outside the scope of the privilege.

Clients may choose to waive privilege in order to cooperate in litigation or with a governmental investigation. Counsel should be aware of this potential strategy and its impact on the future use and protections of documents voluntarily disclosed. To the extent there was a disclosure to a third party (including a governmental or regulatory body), counsel should closely examine the circumstances of the disclosure, such as whether the disclosure was compelled, voluntary, or inadvertent; the scope

83. *See* United States v. Mejia, 655 F.3d 126, 132 (2d Cir. 2011).

of the disclosure; and whether the disclosure was made pursuant to a confidentiality agreement, protective order, or other order of a court or other authoritative body.[84] Factors that may weigh in favor of nonwaiver are that the disclosure was unauthorized, compelled, very limited in scope, and/or made under a confidentiality agreement or court order. For example, in the United Kingdom, a privileged document may be selectively shared with regulators for a defined purpose without necessarily losing its privileged status.[85] By contrast, a broad voluntary disclosure to a third party in the absence of a confidentiality agreement will likely weigh in favor of a finding that there has been a waiver. If the disclosure was inadvertent, counsel should be prepared to clearly articulate how the privilege review protocol was reasonable and appropriate under the circumstances and how counsel acted immediately to retrieve the inadvertently disclosed documents or information.

Finally, to the extent practicable, counsel should avoid putting privileged documents or information directly at issue, such as by arguing that the client acted in good faith based on the client's review of a particular privileged document or legal advice received from counsel, which could waive otherwise applicable privilege. If counsel cannot avoid putting arguably privileged documents or information at issue, counsel should take all reasonable steps to narrow the scope of any waiver, including through negotiating an agreement with the other party or

84. *See* Regents of the Univ. of Cal. v. Super. Court of San Diego Cnty., 81 Cal. Rptr. 3d 186 (Cal. Ct. App. 2008) (finding no waiver of privilege because at the time of the cooperative disclosure "it would not have been reasonable for defendants to resist or otherwise challenge the government's requests").

85. *See* Prop. All. Grp. Ltd. v. The Royal Bank of Scotland Plc [2015] EWHC 1557 (Ch) (UK). Selective waiver is only followed by a minority of U.S. courts. The First, Third, Fourth, Sixth, Ninth, Tenth, and D.C. Circuits all reject the selective-waiver doctrine.

by seeking a protective order or other relief from the court that the use and disclosure of the document will not result in a broad waiver. However, such protection may still fail to protect disclosed information from waiver in other jurisdictions.

F. Practice Point 6: Special Planning is Necessary for Parallel Proceedings and Simultaneous or Sequential Litigation

Counsel should be aware that parallel proceedings and simultaneous or sequential litigation require special planning and cooperation.[86] In international litigation, "parallel proceedings" often refers to the simultaneous pendency of claims between the same or similar parties in the courts of different countries. "Parallel proceedings" also can refer to simultaneous or successive investigations or litigations arising out of a common set of facts, initiated by any combination of criminal, civil, or administrative authorities as well as private plaintiffs.

When a parallel proceeding involves an investigation by a foreign regulator or prosecutor, counsel should carefully assess legal privileges on a global scale, as the production of documents otherwise protected from disclosure to a foreign regulator may have multiple ramifications in parallel or successive

86. *See also Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders*, *supra* note 77, at 447–48. "While we believe that, as a general proposition, it is in the best interests of all concerned parties (and authorities) to cooperate on some level and work together to ensure that all matters proceed more or less in tandem, and to ensure that the end results are, if not uniform, at least not inconsistent or mutually exclusive, we also realize that in some situations one or more of the parties may not think that cooperation or coordination is in its own best interest. In those circumstances, it may be incumbent on the presiding tribunals (in the case of litigation) and the responsible government authorities (in the case of investigations) either to "encourage" any reluctant party to cooperate or, where that is not possible, to exercise its powers to maintain progress in its pending matter and prevent any unjustified delay."

proceedings.[87] For example, when evaluating whether to produce a legally privileged document to a foreign regulator voluntarily to demonstrate cooperation in an investigation, counsel should assess the possibility of and risks associated with subsequent litigation or investigations in other jurisdictions where such production may result in waiver of the privilege over the specific document produced as well as all documents concerning the same subject matter.[88]

To the extent multiple law firms are representing an entity involved in parallel proceedings, their considerations, recommended strategies, and approaches regarding the benefits and risks of disclosing or withholding certain documents should be coordinated as much as practicable.

Simultaneous or sequential proceedings may lead to inconsistent rulings, including inconsistencies regarding whether legal privileges apply to documents at issue. This issue is not unique to matters involving cross-border privilege concerns. Counsel should consider various options to mitigate the risks of

---

87. *See* The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices*, 19 SEDONA CONF. J. 557 (2018) (providing practical guidelines for investigations that require the transfer of protected data across national borders). Principle 3 provides that "Courts and Investigating Authorities should give due regard both to the competing legal obligations, and the costs, risks, and burdens confronting an Organization that must retain and produce information relevant to a legitimate Government Investigation, and the privacy and data protection interests of Data Subjects whose personal data may be implicated in a cross-border investigation."

88. *See, e.g.*, Permian Corp. v. United States, 665 F.2d 1214. 1221 (D.C. Cir. 1981) (privilege should not allow a party to "pick and choose among his opponents, waiving the privilege for some and resurrecting the claim of confidentiality to obstruct others"); United States v. Massachusetts Institute of Technology, 129 F.3d 681 (1st Cir. 1997) (privilege was waived for documents disclosed to a government agency); *In re* Pac. Pictures Corp., 679 F.3d 1121 (9th Cir. 2012) (rejecting selective-waiver doctrine).

inconsistent privilege rulings to the extent they are available, depending on where the proceedings have occurred or are pending.[89] In the United States, this may include seeking to transfer, consolidate, or coordinate matters pending in different courts. It also may include requesting a stay on certain discovery if another forum is better suited to evaluating the applicable privileges and discovery procedures.

Courts have multiple options within their discretion to exercise when confronted with the possibility of inconsistent rulings in simultaneous proceedings for matters pending in multiple jurisdictions. They may choose to do nothing and continue to press ahead with the matter(s) before them, reflecting a preference to allow the plaintiff to be permitted to pursue its action in its chosen forum and a reluctance to dismiss or delay a local action over which it has proper jurisdiction and venue. They may raise the possibility of transfer, coordination, or consolidation with the parties and with the judges in other jurisdictions in an effort to not only mitigate the risks of inconsistent rulings but also reduce discovery costs and duplicative motion practice in different courts, thereby conserving party and judicial resources. In the United States, formal statutes and rules may govern transfer, consolidation, and scheduling issues; courts also may rely on their inherent authority to manage litigation before them. Where adjudication of privilege claims over the same documents are simultaneously pending in different jurisdictions, one court may choose to stay or defer ruling on the dispute to allow another court to make its ruling, permitting the other court to analyze the first court's decision and determine whether to follow or depart from it. The two courts may—with

89. *See* Rambus, Inc. v. Infineon Techs. AG, 220 F.R.D. 264 (E.D. Va. 2004) (work-product protection was not waived when documents were produced subject to a court order in a parallel litigation).

the consent of the parties—wish to confer on the procedure to be adopted.

In sequential litigation in different countries or jurisdictions, the parties in the subsequent matter may seek discovery of documents or testimony provided in the initial matter. Counsel and the courts should consider the propriety of such requests and whether the court has the authority to allow for such sharing or productions of documents from foreign proceedings to occur. There may be agreements, protective orders, or confidentiality orders that prevent authorizing access to such documents or testimony. It might be necessary to go back to the original court and request a change in its order(s). In addition, although allowing access or sharing arguably may promote efficiency and cost savings, they may circumvent the scope of permissible discovery in the subsequent proceeding and create unfair or inequitable results.

G. Practice Point 7: Assist Courts with Cross-Border Privilege Issues, as Courts May Lack Familiarity with Relevant Jurisdictional Laws

Counsel can responsibly assist courts, regulators, and others with understanding and navigating privilege and other protection issues in multijurisdictional matters. Counsel is accountable for understanding the applicable rules and practices concerning the discretion afforded courts in determining issues of privilege. Counsel bears the burden of demonstrating that a foreign jurisdiction's law is applicable, and the documents or information in question fall under those laws.

In civil litigation in U.S. federal courts, Federal Rule of Civil Procedure 26(f) requires litigants to meet and confer early in the litigation process and propose a discovery plan. Rule 26(f)(3)(B) and (D) require that the parties address these topics in their discussions leading to their proposed discovery plan: "(B) the

subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused on particular issues;" and "(D) any issues about claims of privilege or of protection as trial-preparation materials, including—if the parties agree on a procedure to assert these claims after production—whether to ask the court to include their agreement in an order under Federal Rule of Evidence 502." Parties should use these required early conferences to present an informative plan to the court and to flag issues, including cross-border privilege issues, that may become larger disputes at a later point.

Where parties and their counsel are aware early in the lawsuit that discovery may implicate the privilege laws of non-U.S. jurisdictions, Rule 26(f)'s required meet-and-confer discussions and discovery plan provide an opportunity for parties and their counsel to raise and potentially reach agreement regarding the need and approach for addressing such documents. This may include, among other topics, reaching agreements regarding the privileged or protected nature of the documents, the scope of their discovery, and whether a phased approach to the potential production of such documents may be appropriate. A phased approach, focusing, for example, first on U.S. documents and information, might avoid the potential for protracted disputes regarding the application of non-U.S. jurisdictions' privileges if, after the discovery of U.S. documents, non-U.S. materials are only marginally relevant to the parties' claims and defenses (and therefore may not require production). Discovery focused on non-U.S. materials at the outset may then be disproportionate to the litigation if the parties can obtain adequate discovery from other sources or means that do not implicate cross-border privilege issues.[90]

90. *See, e.g.*, FED. R. CIV. P. 26(b)(1) and (f)(3).

Although less frequently invoked, Federal Rule of Civil Procedure 44.1 also is instructive if the non-U.S law issue arises later in the lawsuit, if the parties dispute whether non-U.S. law applies, or if the parties dispute how non-U.S. law affects the discoverability of the documents and information at issue. Rule 44.1 not only requires that the parties provide notice of their intent to raise an issue about non-U.S. law, it also provides guidance to the court regarding what sources the court may use to adjudicate the non-U.S. law and states that the determination is a question of law, not a question of fact. Specifically, Rule 44.1 states:

> A party who intends to raise an issue about a foreign country's law must give notice by a pleading or other writing. In determining foreign law, the court may consider any relevant material or source, including testimony, whether or not submitted by a party or admissible under the Federal Rules of Evidence. The court's determination must be treated as a ruling on a question of law.

The Federal Rules of Civil Procedure also permit the court to appoint a special master or an expert to assist the court in its determination of the non-U.S. law.[91]

The 1966 Advisory Committee Notes highlight the court's flexibility in determining the applicability of non-U.S. laws. They state that the court "may engage in its own research and consider any relevant material thus found. The court may have at its disposal better foreign law materials than counsel have presented, or may wish to reexamine and amplify material that has been presented by counsel in partisan fashion or in

91. *See, e.g.*, FED. R. CIV. P. 53 (appointing special masters) and FED. R. EVID. 706 (court-appointed expert witnesses).

insufficient detail. On the other hand, the court is free to insist on a complete presentation by counsel." The Advisory Committee Notes further state that "the rule provides flexible procedures for presenting and utilizing material on issues of foreign law by which a sound result can be achieved with fairness to the parties." If the court engages in its own research, it is not obligated to provide notice to the parties; however, the Advisory Committee Notes encourage that, ordinarily, "the court should inform the parties of material it has found diverging substantially from the material which they have presented; and in general the court should give the parties an opportunity to analyze and counter new points upon which it proposes to rely."

When issues arise in discovery regarding the applicability in federal courts of non-U.S. privileges or other protections, such as confidentiality or professional secrecy obligations, in practice the parties often submit declarations or affidavits from experts regarding the non-U.S. law and the discoverability of the documents or information in dispute.[92] The parties also may submit translations of non-U.S. laws or non-U.S. court opinions that may be relevant to the court's determination of the applicable law regarding privileges and discoverability.

To assist the court in its determination of non-U.S. law, counsel should proactively compile relevant treatises, laws, court opinions, and authorities. Counsel also should identify potential experts who are qualified to credibly address the non-U.S. laws and their application to the documents or information in dispute.

---

92. Note that, although Federal Rule of Civil Procedure 26(b) as amended in 2010 provides some protection against disclosure, documents and materials provided to testifying experts and drafts of their reports may still be discoverable in U.S. litigation, even if they contain otherwise privileged information. *See, e.g.*, *In re* Application of the Republic of Ecuador, 735 F.3d 1179 (10th Cir. 2013); *In re* MTBE Prods. Liab. Litig., 293 F.R.D. 568 (S.D.N.Y. 2013).

H. Practice Point 8: Understand Applicable Choice-of-Law and Comity Principles

Counsel should comprehend and evaluate the forum jurisdiction's choice-of-law rules, including the forum's recognition and implementation of comity principles. Where appropriate, counsel should advocate for a choice-of-law analysis that applies the privilege law of the jurisdiction with the most compelling interest in whether the putatively privileged information remains confidential.

Common law countries have traditionally based choice-of-law analyses on whether the dispute at issue is procedural or of substantive law. If the dispute involves a procedural issue, then the jurisdiction typically follows the *lex fori*, or law of the forum, approach. But if the dispute involves a matter of substantive law, then the jurisdiction, applying comity principles, evaluates whether to apply the law of the jurisdiction with the most compelling interest in the legal matter at issue.

The principle of comity, in a traditional sense, is one of courtesy arising from a general disposition to accommodate.[93] In a legal sense, comity is "the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens, or of other persons who are under the protection of its laws."[94] Comity is not an absolute obligation or a rule of law. Rather, it is a principle of convenience, expediency, and "due respect" under which courts apply another country's law if doing so does not violate

93. Disconto Gesellschaft v. Terlinden, 106 N.W. 821 (Wis. 1906).

94. Hilton v. Guyot, 159 U.S. 113 (1895); McFarland v. McFarland, 19 S.E.2d 77 (Va. 1942); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 101 (AM. LAW INST. 1987).

the forum country's public policy or prejudice the rights of its citizens.[95]

In the disclosure protection law context, some common law countries, such as the United Kingdom, apply the *lex fori* approach to cross-border privilege disputes even though they recognize privilege law as substantive in nature. Other countries, such as the United States, recognize privilege law as substantive and apply various versions of a comity-based, most-compelling-interest test. Still other jurisdictions, such as Canada, traditionally have applied the *lex fori* approach to what the courts viewed as procedural-based privilege law but have since recognized as substantive, leaving the choice-of-law analysis open to further clarification.

Whether the jurisdiction considers privileges as procedural or substantive, counsel should nevertheless evaluate whether and how comity principles should affect a court's determination of which privilege law to apply to a cross-border disclosure dispute. The Sedona Conference has suggested that courts apply comity principles in other information-protection contexts[96] and continues that guidance in the context of cross-border privilege disputes. To the extent practicable under the circumstances, counsel should advocate for and courts should consider, as recommended below in Section IV, a comity-based choice-of-law analysis that applies the privilege law of the jurisdiction with

95. *Hilton*, 159 U.S. at 163–65 (stating comity is not an "absolute obligation" nor "mere courtesy and good will"); Mast, Foos & Co. v. Stover Mfg. Co., 177 U.S. 485, 488 (1900) (stating comity is not a rule of law but one of practice, convenience, and expediency); Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for S. Dist. of Iowa, 482 U.S. 522, 546 (1987) (stating that American courts should "demonstrate due respect" for issues that foreign litigants confront).

96. *See Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders*, *supra* note 77, at 404–06; *Sedona Conference International Litigation Principles*, *supra* note 74, at 9–10.

the most compelling interest in whether the putatively protected information remains confidential, unless that law violates the forum's public policy or otherwise prejudices the rights of those within its jurisdiction.

To preemptively deal with choice-of-law issues and minimize the risk that another jurisdiction's privilege laws will apply to documents or information, counsel should consider including, and carefully negotiate, forum-selection and choice-of-law provisions in their clients' contracts, including in mandatory arbitration provisions. In 2013, for example, the Supreme Court of the United States confirmed deference to forum-selection clauses in *Atlantic Marine Construction Co. v. United States District Court for the Western District of Texas*, explaining that when "parties have contracted in advance to litigate disputes in a particular forum, courts should not unnecessarily disrupt the parties' settled expectations." Counsel should ensure that choice-of-law provisions specify the chosen jurisdiction's disclosure protection laws, including evidentiary privileges and the work-product doctrine.[97]

97. In *Hercules, Inc. v. Martin Marietta Corp.*, 143 F.R.D. 266 (D. Utah 1992), the court held that Utah's accountant-client privilege applied even though the parties' contract called for application of Colorado law. The court determined that the choice-of-law provision governed "the contract" and that "[n]othing in the express terms of the contract applies to the law of privileged communications."

IV. RECOMMENDED CHOICE-OF-LAW ANALYSIS

Documents or information protected from disclosure in one jurisdiction may not receive the same disclosure protection in another jurisdiction. When this conflict-of-laws issue arises, the jurisdiction in which the dispute is pending must apply its choice-of-law rules to determine whether its protection law or another country's protection law governs the disclosure dispute. In jurisdictions where the choice of privilege law analysis remains an open question or lacks uniformity, counsel should advocate for, and courts should consider applying, a comity-based approach. This approach is one in which the privilege law of the jurisdiction with the most compelling interest in whether the documents or information at issue remain confidential is selected. Recent Sedona Conference Choice of Law Principles regarding personal data support this approach.[98] Choice of Law Principle 4, for example, recognizes that "a person's choice of jurisdiction or law should not deprive him or her of protections that would otherwise be applicable to his or her data."[99] Choice of Law Principle 6 advocates for the protection of personal data in the context of litigation and investigations in that "such data shall be provided when it is subject to appropriate safeguards that regulate the use, dissemination, and disposition of the data."[100] An exception to the application of such a comity-based approach would be if applying a foreign jurisdiction's privilege law, or acknowledging that jurisdiction's confidentiality and professional secrecy obligations, would violate fundamental

98. *Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders*, *supra* note 77.

99. *Id.* at 435. "Principle 4 recognizes that every affirmative choice of jurisdiction or law may imply a derogation of protections and standards that may be considered unacceptable by another jurisdiction . . . ."

100. *Id.* at 441.

public policy, or other fundamental rights, such as individual rights, in the forum.

Courts in some common law countries apply the law of the forum—*lex fori*—approach, which typically derives from the fact that courts in those jurisdictions treated the application of a privilege or other protection as a procedural matter. Courts in other common law jurisdictions, by contrast, determine cross-border privilege disputes using a multifactor choice-of-law analysis. Those jurisdictions often consider the application of a privilege as a matter of substantive law rather than as a procedural matter.

A. United Kingdom

Courts in the United Kingdom typically follow the *lex fori* approach and apply the forum's privilege law when there is a conflict of privilege laws in cross-border proceedings.[101] As previously discussed in Section II.A.9, the English court established this rule in *Lawrence v. Campbell*.[102]

Though the *lex fori* approach often traces its roots to the view that the attorney-client privilege is a matter of procedure and not a matter of substantive law, courts have not focused their analysis on that dichotomy. In *Re Duncan*, for example, the English court applied the forum's solicitor-client privilege between

---

101. GIBSON DUNN, ARE WE SPEAKING THE SAME LANGUAGE? PRIVILEGE ISSUES IN CROSS-BORDER LITIGATION, INVESTIGATIONS, AND INTERNATIONAL ARBITRATION 6 (May 16, 2017), *available at* https://www.gibsondunn.com/webcast-are-we-speaking-the-same-language-privilege-issues-in-cross-border-litigation-investigations-and-international-arbitration/.

102. [1859] Eng. Rep. 385. "A question has been raised as to whether the privilege in the present case is an English or Scotch privilege; but sitting in an English Court, I can only apply the English rule as to privilege, and I think the English rule as to privilege applies to a Scotch solicitor and law agent practicing in London, and therefore the letters in question are privileged from production."

a domestic client and foreign counsel without basing its ruling on finding that the privilege is a procedural matter. Rather, the court pointed to a more practical consideration—the complexity involved in determining another jurisdiction's privilege law. Deciding to apply *lex fori*, the English court stated that "any other conclusion would lead to an impossible position for if this court were required to investigate the position of such communications in foreign law it must first determine the foreign law."[103]

In the 2016 *RBS Rights Issue Litigation*, the English court again upheld the longstanding *Lawrence* rule, applying *lex fori* doctrine in resolving a privilege issue in a cross-border proceeding.[104] There, the Royal Bank of Scotland (RBS) argued that the court should apply the privilege law of the United States, the jurisdiction most closely connected to the communications at issue.[105] RBS argued that the traditional rule imposing the forum's law on privilege questions was obsolete, because courts now recognized the legal professional privilege as a substantive right rather than a procedural rule of evidence.[106] The court rejected this "bold submission" and found "no sufficient basis" to disturb the well-established *lex fori* approach,[107] explaining that "it would be altogether too drastic and unsupported departure to adopt an entirely new ''choice of law rule.'" RBS's proposed rule would have applied the law of the jurisdiction most closely connected to the engagement or instructions under which the putatively privileged documents came into existence, unless that jurisdiction's law was contrary to English public policy. The court

103. *Re* Duncan, [1968] 2 W.L.R. 1479 (Can.).

104. [2016] EWHC (Ch) 3161 [174] (Eng.).

105. *Id.* at 145.

106. *Id.* at 147.

107. *Id.* at 148.

identified this proposed rule as the most-significant-relationship test that many U.S. courts apply. The court found the proposed rule counterintuitive because it would start by subordinating English public policy—the *lex fori* policy—to the laws of another jurisdiction only to allow English public policy to be reasserted if the foreign jurisdiction's law departed too far from the *lex fori* approach.

The English court remained true to the *lex fori* approach even though it doubted that courts ever based this rule on the privilege's classification as substantive or procedural. Rather, the court stated that the forum law approach was a decided public policy, and even recognizing a privilege as a substantive right did not justify departing from the well-settled rule. The court noted that an alternative rule would be difficult to implement. The court also did not see its adherence to the *lex fori* rule as "hostile to comity" because this rule is the implementation of public policy.

Still, the English court indicated the possibility that exceptions to the *lex fori* rule could exist through the court's "discretionary override."[108] A statute provides courts with the ability to prevent disclosure even if unprotected by the forum's privilege law where the disclosing party proves a "right or duty" to withhold disclosures. Although the court recognized that the "right or duty" could be foreign law, it said that parties have a higher hurdle where the foreign law is an expectation of confidentiality and the forum's law is based on public policy.

B. United States

United States federal courts apply comity principles to varying degrees in addressing cross-border privilege disputes. Courts in the Second Circuit, for example, apply a "touch base"

108. *Id.* at 174.

analysis that includes a comity element.[109] This standard centers on whether the United States or another country has the predominant or most direct or compelling interest in whether putatively privileged communications remain confidential.[110] These courts apply U.S. privilege law to communications that "touch base" with the United States. But, as a matter of comity, courts apply another country's privilege law when the communications relate "solely" to the other country unless the other country's law is contrary to U.S. public policy.[111] "Communications concerning legal proceedings in the United States or advice regarding United States law are typically governed by United States privilege law, while communications relating to foreign legal proceedings or foreign law are generally governed by foreign privilege law."[112]

Even where courts have not strictly applied the touch-base analysis, the factors courts examine in undertaking that analysis have informed decisions on application of a privilege. For example, in *Astra Aktiebolag v. Andrx Pharmaceuticals, Inc.*,[113] the

109. *See* Mangouras v. Squire Patton Boggs, 980 F.3d 88, 98–99 (2nd Cir. 2020) (noting that "touch base" is a "traditional choice-of-law ''contacts' analysis to determine the law that applies to claims of privilege involving foreign documents" and recognizing the "touch base" test as the "proper choice-of-law test for purposes of determining" legally applicable privileges in the § 1782 context).

110. Astra Aktiebolag v. Andrx Pharm., Inc., 208 F.R.D. 92, 98–99 (S.D.N.Y. 2002); Golden Trade, S.r.L. v. Lee Apparel Co., 143 F.R.D. 514, 518–19 (S.D.N.Y. 1992).

111. Veleron Holding, B.V. v. BNP Paribas SA, No. 12-CV-5966 (CM)(RLE), 2014 WL 4184806, at *4 (S.D.N.Y. Aug. 22, 2014); Gucci Am., Inc. v. Guess?, Inc., 271 F.R.D. 58, 64–65 (S.D.N.Y. 2010); Bayer AG & Miles, Inc. v. Barr Labs., Inc., 1994 WL 705331, at *3–4 (S.D.N.Y. Dec. 16, 1994).

112. Anwar v. Fairfield Greenwich Ltd., 982 F.Supp.2d 260, 264 (S.D.N.Y. 2013).

113. *Astra Aktiebolag*, 208 F.R.D. at 96–99.

court determined that under the touch-base test different countries' privilege laws applied to different documents. The court found that Korean law applied to certain documents and determined that the documents were not protected by privilege under Korean law.[114] However, the court also observed that the documents in question would have never been discoverable in the first instance in Korean litigation.[115] Because the application of Korean privilege law would "require disclosure of many documents (1) that are protected from disclosure under American law and (2) that would not be discoverable under Korean law," the court ultimately decided to apply U.S. privilege law, even though the communications did not "touch base" with the United States.[116] The court then concluded that certain documents were privileged under U.S. law, including a communication between the company and its outside Korean counsel.[117]

The *Wultz* court narrowly cabined the *Astra* court's approach.[118] In *Wultz,* the party resisting discovery relied upon *Astra* to argue that Chinese law should not apply to certain documents, because American-style discovery would never occur in

114. *Id.* at 100–02.

115. *Id.* at 101 ("However, both of these findings—lack of a statutory attorney-client privilege and work product protection in Korea—rest on the assumption that parties may be ordered or required to testify or produce documents concerning confidential communication by a Korean court during a lawsuit. The court finds that such an assumption is, in fact, erroneous. Astra has demonstrated sufficiently for the purposes of this court's present document review that these documents would not be subject to production, whether through a discovery process or by court order, in a Korean civil lawsuit.").

116. *Id.* at 102.

117. *Id.* at 104–05.

118. Wultz v. Bank of China Ltd., 979 F. Supp. 2d 479 (S.D.N.Y. 2013).

China.[119] Nevertheless, the court applied Chinese law to certain documents.[120] For the *Wultz* court, the fact that information theoretically was discoverable under Chinese law was sufficient to distinguish *Astra* and find that the documents were not privileged.

Courts in the Seventh Circuit, by contrast, and at least in the patent agent context, avoid the touch-base approach[121] and apply a comity functionalism approach under which comity

---

119. *Id.* at 490. *See also* Gucci America, Inc. v. Guess?, Inc., 271 F.R.D. 58, 65 (S.D.N.Y. 2010) ("[C]ommunications relating to legal proceedings in the United States, or that reflect the provision of advice regarding American law, 'touch base' with the United States and, therefore, are governed by American law, even though the communication may involve foreign attorneys or a foreign proceeding.").

120. *Id.* at 490–91 ("*Astra* does not stand for the proposition that principles of comity forbid the application of foreign privilege law of any jurisdiction where discovery practices are more circumscribed than in the United States. . . .

The critical inquiry in *Astra* is not whether the disclosure of attorney-client communications *would* happen, but rather whether it *could* happen. The court in *Astra* made clear that the documents at issue could not be produced under the specific limited circumstances designated by statute and the opposing party had no independent legal right to the documents under Korean law.

Here, even [the expert of the party resisting discovery] admits [t]here are general provisions in [Chinese] law that allow judges to compel parties to provide certain information under certain circumstances. . . . [N]othing in Chinese law prevents the disclosure of these documents in the same way that Korean law prevented the disclosure of the documents in question in *Astra*. . . . Because attorney-client and work product communications and documents could be subject to discovery under Chinese law, applying Chinese privilege law does not violate principles of comity or offend the public policy of this forum.").

121. Baxter Int'l, Inc. v. Becton, Dickinson & Co., No. 17 C 7576, 2019 WL 6258490, at *2 (N.D. Ill. Nov. 22, 2019) (stating that "Courts in this District have decided to forego the 'touching base' test").

principles drive the choice-of-law analysis rather than just serve as an element of the evaluation. In *SmithKline Beecham Corp. v. Apotex Corp.*,[122] the court applied a two-pronged test to determine whether the attorney-client privilege protected communications between a client and its United Kingdom patent agents. As a matter of comity, the court first looked to whether English law supplied privilege protection to patent agent communications. Second, the court examined the function that the patent agents were performing to determine whether they were "engaged in the substantive lawyering process."[123] From a choice-of-law standpoint, the court stated that, "as a matter of comity, and as a functional approach to the problem, the trend is for courts to look to the foreign nation's law to determine the extent to which the privilege may attach."[124] Applying that analysis, the court determined that under English law, patent agent work was protected, as they more or less functioned as attorneys, and that confidential legal advice should remain privileged.[125] As a

122. No. 98 C 3952, 2000 WL 1310668 (N.D. Ill. Sept. 13, 2000).

123. *Id.* at *2.

124. *Id. See also* McCook Metals, LLC v. Alcoa, Inc., 192 F.R.D. 242, 256 (N.D. Ill. 2000) (stating that "if an attorney-client privilege exists in a country, then comity requires us to apply that country's law to the documents at issue"); *Baxter Int'l*, 2019 WL 6258490, at *2 (applying Swedish law to determine whether the attorney-client privilege applied to communications providing legal advice to a Swedish company).

125. *See also* Golden Trade, S.r.L. v. Lee Apparel Co., 143 F.R.D. 514, 520 (S.D.N.Y. 1992) ("[C]ommunications by a foreign client with foreign patent agents 'relating to assistance in prosecuting patent applications in the United States' are governed by American privilege law whereas communications 'relating to assistance in prosecuting patent applications in their own foreign country' or 'rendering legal advice . . . on the patent law of their own country' are, as a matter of comity, governed by the privilege 'law of the foreign country in which the patent application is filed,' even if the client is a party to an American lawsuit.").

result, the court ruled that the party's communications with British patent agents were protected from disclosure.

Taken together, these brief examples demonstrate that it is difficult to predict with certainty what laws of privilege U.S. courts will apply, even when the courts are operating within the District or Circuit. However, the touch-base approach gives courts the necessary flexibility to determine a fair path through discovery snarls involving documents and information from multiple countries and to determine privilege questions after giving due consideration to various interests.

C. Canada

Canadian courts, citing the English *Lawrence* and *Duncan* decisions, typically apply the *lex fori* approach to disclosure disputes concerning communications with or materials prepared by foreign lawyers. Many of these decisions simply decided whether Canada's solicitor-client privilege applied to communications involving foreign counsel without determining whether the forum's law applied (because of the procedural-substantive dichotomy) and without setting forth the specific factors the court considered in reaching the result.[126]

While Canadian courts generally apply the country's privilege law even when the putatively privileged communications involve foreign counsel, the Supreme Court of Canada has not addressed the conflict of privilege laws issue. Nor has there been a consistent body of case law setting forth the factors courts employ in selecting the privilege law to apply or the rationale

126. *See, e.g.*, Morrison-Knudsen Co. v. British Columbia Hydro & Power Auth. (1971), 19 D.L.R. 3d 726 (citing *Lawrence* and *Duncan* in applying Canada's solicitor-client privilege to communications between U.S. lawyers and a U.S. corporation without addressing whether privilege was substantive or procedural or whether U.S. privilege law governed).

underlying those decisions. As a result, Canada's preferred choice-of-law analysis for privileges is unsettled.[127]

Indeed, authority exists to support a choice-of-law analysis that involves principles of comity rather than strict adherence to *lex fori*. First, Canadian courts' definition of comity mirrors the definition given by the Supreme Court of the United States in *Hilton v. Guyot*.[128] Comity plays an important role in courts' *forum non conveniens*[129] analyses and, generally, in enforcing letters rogatory seeking discovery for use in a foreign jurisdiction.[130] Second, while the solicitor-client privilege's "historical roots are a rule of evidence," indicating that it is procedural in nature, courts frequently identify the privilege as a "fundamental right" and a "substantive rule of law."[131]

Canadian courts' application of comity principles and recognition that privileges are substantive in nature offer a basis for lawyers to advocate for a comity-based choice-of-law analysis. These maxims were on display in *Glegg v. Glass*,[132] where the court identified the solicitor-client privilege as a substantive rule of law and applied traditional comity principles to reject a Florida court's request for the deposition of a Canadian solicitor. The court stated that as a matter of comity, courts will give effect to the laws of another jurisdiction "out of mutual deference and respect," unless it is contrary to Canada's public policy. The court then identified Canada's solicitor-client privilege

127. Brandon Kain, *Solicitor-Client Privilege and the Conflict of Laws*, 90 CAN. B. REV. 243, 252–53 (2011), *available at* https://cbr.cba.org/index.php/cbr/article/view/4270.

128. Morguard Invs. Ltd v. De Savoye, [1990] 3 S.C.R. 1077 (quoting Hilton v. Guyot, 159 U.S. 113 (1895)).

129. Panniccia v. MDC Partners, Inc., 2017 ONSC 7298.

130. Glegg v. Glass, 2019 ONSC 6623.

131. R. v. McClure [2001] 1 S.C.R. 445.

132. 2019 ONSC 6623.

as a substantive rule of law and held that the Florida court's request for discovery from a solicitor would violate this substantive rule of law and was therefore contrary to Canada's public policy.

D. Australia

Australia applies the *lex fori* approach in determining whether the legal professional privilege protects documents and information from disclosure. In *Stewart and Others v. Australian Crime Commission*,[133] the court faced the issue whether Australian or California law protected documents from discovery. The court stated that the first inquiry is whether privilege exists, and if so, whether it would apply Australian choice-of-law rules to determine whether Australia or California privilege law applied. In making that choice-of-law determination, the court held that "the better argument is that the governing choice-of-law rule for legal professional privilege is the *lex fori*."[134] Its reasons varied and included the fact that English cases follow the *lex fori* approach even though most of these cases, rendered prior to the *RBS Rights Issue Litigation*, were decided when the courts viewed privilege as procedural in nature. The Australian court also noted that privilege is not linked to the theory of liability, such as in contract or tort, but rather is an immunity to otherwise compelled disclosure. Further, legal professional privilege has several "important connecting factors" with the forum, such as the request for and production of documents and the claim and assertion of privilege, and the court

133. [2012] 206 FCR 347.

134. *Id*.

determined that the forum's privilege law governs cross-border privilege disputes.[135]

E. Other Considerations

The touch-base approach has previously been endorsed by the American Law Institute and the International Institute for the Unification of Private Law (UNIDROIT), which originally proposed Rule 24.2 in its preliminary draft of civil procedure rules:

> Evidence cannot be admitted of information covered by other privileges recognized by the law of the place with the most significant relationship to the parties to the communication, unless the court determines that the need for the evidence to establish truth is of greater significance than the need to maintain confidentiality of the information.[136]

In the final version of the UNIDROIT Transnational Principles of Civil Procedure, Rule 24.2 was removed and replaced with the evidentiary privilege and immunities principles. Specifically, 18.1 gives a broader, blander principle that "[e]ffect should be given to privileges, immunities, and similar provisions of a party or nonparty concerning disclosure of evidence or other information."[137]

---

135. *Id.* The court also noted that Australian legal professional privilege "incorporates within it a foreign element," which the court appears to have deemed sufficient to protect other country's interests.

136. Am. Law Inst. & UNIDROIT, Preliminary Draft of Transnational Rules of Civil Procedure (2000), *available at* https://www.unidroit.org/english/documents/2000/study76/s-76-02-e.pdf (last visited July 13, 2022).

137. Am. Law Inst. & UNIDROIT, ALI/UNIDROIT Principles of Transnational Civil Procedure Section 18.1 (2006), *available a*t

F. Recommended "Touch Base" Approach

Common law countries regularly consider comity principles and acknowledge that privilege law can be substantive in nature. While certain common law countries continue to follow the entrenched *lex fori* approach for determining choice-of-law issues, the touch-base approach gives courts the flexibility to apply the law of privilege more fairly. Where there is latitude within a jurisdiction, there may be advantages to arguing for the application of the touch-base legal analysis to privilege disputes, including to argue for the acknowledgement of confidentiality or professional secrecy obligations in other jurisdictions when appropriate. Further developing choice-of-law considerations present practitioners and courts with the ripe opportunity to consider the appropriate analytical framework for determining whether to compel a party to disclose putatively protected information in litigation. Even in England, where *lex fori* has been the law since 1859, courts still see merit in recognizing a choice-of-law analysis that deviates from a *lex fori* approach on a case-by-case basis where there are "compelling reasons" of "exceptional concern." The framework provided by the touch-base approach would offer valuable guidance in such circumstances.

A conflict-of-laws analysis grounded in the touch-base approach promotes public policy goals. First, the approach implements the internationally recognized principles of comity.[138]

---

https://www.unidroit.org/instruments/civil-procedure/ali-unidroit-principles (last visited July 13, 2022).

138. Duplan Corp. v. Deering Milliken, Inc., 397 F. Supp. 1146 (D.S.C. 1974) (ruling that applying a foreign country's privilege law to communications pertaining solely to a foreign country implemented "principles of comity"). These public policy goals correspond with The Sedona Conference International Litigation Principles. For example, Principle 1 of the Sedona Conference International Litigation Principles states that "[w]ith regard to data that

This concept permits courts to defer to a foreign jurisdiction's privilege law or other binding protections, "having due regard both to international duty and convenience, and to the rights of its own citizens, or of other persons who are under the protection of its laws."[139] Yet, comity principles embody flexibility because the forum jurisdiction may reject another country's protections if they violate the forum's public policy or harm its citizens. In other words, "[m]echanical or overbroad rules of thumb are of little value; what is required is a careful balancing of the interests involved and a precise understanding of the facts and circumstances of the particular case."[140]

Second, the approach fulfills the communicating parties' reasonable expectations of confidentiality, which leads to the better observance of laws, accepted practices, and the administration of justice. If the rationale for privilege and other disclosure protections is to allow and encourage the free flow of information between a client and the client's counsel, then recognizing foreign protections—even if the same privileges and protections would not be recognized domestically—promotes the goal of encouraging communication between client and counsel. Conversely, refusal to recognize a foreign privilege if the same would not be recognized domestically could chill open communications between client and counsel. Parties communicating with attorneys or other privileged persons in jurisdictions that recognize the privilege or other protections typically expect their discussions to remain confidential. With this

---

is subject to preservation, disclosure, or discovery in a U.S. legal proceeding, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws."

139. Hilton v. Guyot, 159 U.S. 113 (1895); McFarland v. McFarland, 19 S.E.2d 77 (Va. 1942).

140. Golden Trade, S.r.L. v. Lee Apparel Co., 143 F.R.D. 514 (S.D.N.Y. 1992).

expectation, parties provide their counsel with full and frank information so that the attorney, in turn, has a complete evidentiary narrative from which to provide optimal legal advice.[141] An unexpected foreign jurisdiction's compelled disclosure of information created with confidentiality expectations could chill attorney-client communications and thereby reduce the value of counsel's legal advice.[142] This result would fail to "promote broader public interests in the observance of law and administration of justice."[143]

To be sure, the comity-influenced touch-base approach is imperfect. Its application sometimes places significant factual and legal burdens on courts. The forum court would first have to determine, for instance, whether the privilege laws of two (or more) jurisdictions actually conflict. If so, the court must make a factual determination regarding which jurisdiction has the most compelling interest in the putatively protected information. The court next must identify the legal scope of the interested foreign jurisdiction's evidentiary privileges or other disclosure protection doctrines. This determination may come after considering extensive briefing and the opinions of competing legal experts (and/or court-appointed experts). These difficulties "are compounded where, in multi-jurisdictional cases involving several parties, there is the potential for a variety of different putatively applicable laws, and the prospect of having

141. Mohawk Indus., Inc. v. Carpenter, 558 U.S. 100, 108 (2009); Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

142. *See Upjohn*, 449 U.S. at 393 ("But if the purpose of the attorney-client privilege is to be served, the attorney and client must be able to predict with some degree of certainty whether particular discussions will be protected. An uncertain privilege, or one which purports to be certain but results in widely varying applications by the courts, is little better than no privilege at all.").

143. United States v. Jicarilla Apache Nation, 564 U.S. 162, 169 (2011).

to determine them at an interlocutory stage, with cross-examination of experts if there is a disagreement."[144]

While there will always be a chance of inconsistent interpretations of foreign privilege law—based, for example, on different experts, judges, parties, timing, and facts—the disciplining effect of precedent can lead to more predictable outcomes and more functional guiding principles overall. Supporters of the *lex fori* approach will point to the fact that application of the forum's privilege law offers a simple and pragmatic approach to the problem. And while perhaps "mechanical" in application,[145] the *lex fori* approach allows a more consistent, and predictable, application of a well-developed body of privilege law. However, upending confidentiality expectations and allowing the mere selection of the forum to override all other compelling interests in a privilege determination is anachronistic and not in keeping with an increasingly connected world.

It also should be recognized that the exception in the touch-base approach—which allows for the forum law to apply when the foreign law violates the forum's public policy—can lead to circular application of the *lex fori* approach anyway. The *RBS Issues Litigation* court identified this "conundrum" as "unsatisfactory and counter-intuitive."[146] The conundrum arises because the first stage of the touch-base approach subordinates the forum's law to the privilege rules of another jurisdiction when the other jurisdiction has a more compelling interest in the privilege determination; yet, the second stage of the touch-base approach allows for reassertion of the forum's privilege law if applying the law of another country would conflict with the

144. RBS Rights Issue Litig. [2016] EWHC (Ch) 3161 [174] (Eng.).

145. *Golden Trade*, 143 F.R.D. at 514.

146. [2016] EWHC (Ch) 3161 [174].

forum's public policy.[147] This public policy exception conundrum echoes U.S. Supreme Court Justice Joseph Story's criticisms:

> [Comity] is the most appropriate phrase to express the true foundation and extent of the obligation of the laws of one nation within the territories of another. It is derived altogether from the voluntary consent of the latter, and is inadmissible, when it is contrary to its known policy, or prejudicial to its interests. Thus, comity was subject to what became known as the "public policy exception." Although the public policy exception is arguably necessary to prevent potentially absurd judgments, the exception is self-defeating because a judge is always free to offer some domestic policy that is offended by the foreign law. As one commentator has criticized, "comity and the public policy exception rationales . . . . . lack both analytical structure and standards for determining when and how they should be applied." The result is that a court can always apply the law of the forum state regardless of any foreign interest, however important.[148]

Weighing all considerations, on balance, a comity-based choice-of-law analysis that considers which jurisdiction has the most compelling interest is preferable to the *lex fori* approach in

147. Id.

148. JOSEPH STORY, COMMENTARIES ON THE CONFLICT OF LAWS (7th ed. 1872), *quoted in* Daiske Yoshida, *The Applicability of the Attorney-Client Privilege to Communications with Foreign Legal Professionals*, 66 FORDHAM L. REV. 209 (1997).

cross-border privilege disputes. The touch-base approach applied in the majority of U.S. federal courts exemplifies this standard. The touch-base approach has a more fully developed framework for application through existing use and case law than the "comity functionalism" approach used by some U.S. courts, making the touch-base approach more readily applicable to a variety of complex privilege-conflict situations, such as those involving multiple foreign jurisdictions. In contrast to the *lex fori* standard, the touch-base approach better implements a complete choice-of-law analysis by applying the law that promotes the parties' reasonable expectations of confidentiality. Upholding the confidentiality expectations implements the strong, commonly held public policy of legal compliance and the administration of justice by encouraging parties to speak freely and candidly with their counsel so that counsel provides unimpeded legal advice. The approach also more fully executes comity principles by not obligating courts to apply foreign privilege law and allowing the forum's public policies to override foreign privilege law that may otherwise apply. So, while in some cases applying the touch-base analysis can lead to the same conclusion had the court applied *lex fori* from the start, allowing courts to weigh all of the factors and interests in performing the analysis will lead to fairer and more practical determinations that are in keeping with the fundamental policies underlying the attorney-client privilege and other disclosure protections.

V. APPENDIX: COMMON LAW AND CIVIL LAW EXEMPLAR JURISDICTIONS[149]

A. Common Law Exemplar Jurisdictions

1. Australia

Australia's Federal Court Rules provide the general scope of discovery in the country's federal courts.[150] In the Federal Court of Australia, discovery is not required unless the court orders it,[151] and a party should not apply for an order of discovery unless it will facilitate the "just resolution of the proceeding as quickly, inexpensively and efficiently as possible."[152] A party providing discovery without a court order is not entitled to any costs or disbursements for providing the discovery.[153] There are also rules regarding "preliminary discovery" wherein prospective applicants can apply for a court order to discover documents when the prospective applicant reasonably believes he or she may have the right to obtain relief from a prospective respondent but does not have sufficient information.[154]

Discovery under the Australian Federal Court Rules consists of "documents that are directly relevant to the issues raised by

149. The coverage of country specific information here is necessarily limited by the scope of the *Commentary*. For additional information on other countries, we recommend as a starting point DLA Piper's regularly updated Global Guide to Legal Professional Privilege, *available at* https://www.dlapiperintelligence.com/legalprivilege/.

150. *See generally Federal Court Rules 2011* (Cth) (Austl.) (May 21, 2019 update), *available at* https://www.legislation.gov.au/Details/F2019C00426. There are separate discovery rules for the state courts. For example, Part 21 of the New South Wales Uniform Civil Procedure Rules 2005.

151. *Federal Court Rules 2011*, Rule 20.12 (1).

152. *Id.*, Rule 20.11.

153. *Id.*, Rule 20.12 (2).

154. *Id.*, Rule 7.21 et seq.

the pleadings or in the affidavits," "of which, after a reasonable search, the party is aware," and "that are, or have been, in the party's control."[155] These documents must be those on which the party intends to rely, documents adversely affecting the party's own case, document's supporting another party's case, or documents adversely affecting another party's case.[156] In order to be considered a "reasonable search," a party must take into account the nature and complexity of the proceeding, the number of documents involved, the ease and cost of retrieving a document, the significance of any document likely to be found, and any other relevant matter.[157]

The Federal Court Rules specify that a discovery order "does not require the person against whom the order is made to produce any document that is privileged."[158] The producing party must provide a list of documents that must describe "each document in the party's control for which privilege from production is claimed and the grounds of this privilege."[159]

Legal professional privilege protects communications between lawyers and their clients. More specifically, "client legal privilege" or "legal professional privilege" in Australia consists of two distinct types: "advice privilege" and "litigation privilege."[160] Advice privilege protects legal advice given by a

155. *Id.*, Rule 20.14(1).

156. *Id.*, Rule 20.14(2).

157. *Id.*, Rule 20.14(3).

158. *Id.*, Rule 20.02.

159. *Id.*, Rule 20.17(2)(c).

160. *Client Legal Privilege*, LAW COUNSEL OF AUSTRALIA, https://www.lawcouncil.asn.au/policy-agenda/regulation-of-the-profession-and-ethics/client-legal-privilege (last visited July 13, 2022); *see also* Aaron Alcock, *Legal Professional Privilege*, HOPGOODGANIM (July 3, 2019), https://www.hopgoodganim.com.au/page/knowledge-centre/fact-sheets/legal-professional-privilege.

lawyer to his or her client.[161] Litigation privilege protects communications between a lawyer and a client (or third party) about actual or contemplated litigation or court proceedings.[162] For the Federal Court of Australia, these privileges are enshrined in Sections 118 and 119 of the Evidence Act 1995.[163]

The client can waive the privilege, but the lawyer cannot.[164] When determining whether the privilege covers a communication, Australian courts utilize the "dominant purpose test" (i.e., the dominant purpose of the communication was to provide the client with professional legal services).[165] The court employs an "inconsistency test," which looks at inconsistency between the conduct of the client and the maintenance of the confidentiality, to determine whether the client has waived privilege.[166]

Legal professional privilege in Australia has its limits. The Federal Court has held that privilege does not apply to communications made to facilitate an illegal or improper purpose.[167]

---

161. *Id*.

162. *Id*.

163. *Evidence Act 1995*, *available at* https://www.legislation.gov.au/Details/C2018C00433. Similar or identical provisions have been adopted in New South Wales (see *Evidence Act 1995* (NSW)) and Tasmania (see *Evidence Act 2001* (Tas)).

164. Australian Government, Australian Law Reform Commission, *Client legal privilege* (Aug. 17, 2010), https://www.alrc.gov.au/publication/uniform-evidence-law-alrc-report-102/14-privileges-extension-to-pre-trial-matters-and-client-legal-privilege/client-legal-privilege/.

165. Esso Australia Resources v Commissioner of Taxation [1999] 201 CLR 49 (Austl.).

166. *See Mann v. Carnell,* [1999] HCA 66. The court stated that it is the client who is entitled to the benefit of professional confidentiality, and the client may relinquish that entitlement. *Id.* at 26.

167. *See Aucare Dairy Pty. Ltd. v. Huang* [2017] FCA 746, [10]. The Court further held that the applicants did not need to prove that the respondent's

Professional privilege is further limited to admitted solicitors with a right to practice.[168] Similar to other jurisdictions, the Australian courts have determined that in-house counsel may not be sufficiently "independent" for communications with their corporate employer clients to be privileged, though decisions have not been categorical, and there thus remains flexibility to argue that circumstances in a particular case demonstrate the requisite "independence" has been shown such that the privilege applies.[169] Finally, legal professional privilege can be used to resist compelled production but will not entitle the privilege holder to a remedy, such as restraining the use of privileged documents.[170]

---

solicitors had knowledge of or participated in the fraud in order to succeed in their application.

168. *See Vance v. Air Marshall McCormack* [2004] ACTSC 78. The court held at that, absent practicing certificates or the supervision of others with practicing certificates, the requirements for privilege would not be satisfied unless the solicitors enjoyed a statutory right to practice such as provided by the Judiciary Act.

169. *See Telstra Corp Ltd v. Minister for Communications, Information Technology and the Arts* (No. 2) [2007] FCA 1445. Judge Peter Graham stated that, in his opinion, an in-house lawyer will lack the requisite measure of independence if his or her advice is at risk of being compromised by virtue of the nature of his or her employment relationship with the employer. However, the court did leave open the opportunity for in-house counsel to meet the requisite level of independence by stating "[o]n the other hand, if the personal loyalties, duties and interests of the in-house lawyer do not influence the professional legal advice which he gives, the requirement for independence will be satisfied."

170. *Glencore International AG v. Commissioner of Taxation of the Commonwealth of Australia* [2019] HCA 26, [5]. The documents at issue were created for the sole or dominant purpose of obtaining legal advice but were stolen and provided to the International Consortium of Investigative Journalists and subsequently obtained by the Australian Taxation Office [ATO]. The court held that the documents were exempt from production by court process or statutory compulsion, but this declaration would not assist Glencore

As far as confidentiality of documents, Australian courts will generally attempt to fashion protective orders that balance the competing interests of the party seeking production and the privacy or commercial interest of the party claiming confidentiality.[171] While parties can negotiate a confidentiality agreement instead of relying on the courts to fashion an order,[172] courts are willing to order protection of confidential information. This may involve an individual inspecting the documents to execute express confidentiality undertakings, restricting the inspection of the documents to specified persons (such as a legal professional), redacting or editing the documents, or other protective measures that the court deems necessary.[173]

2. Canada

Discovery procedure in Canada is generally governed by the various provinces' rules of civil procedure, which are relatively uniform. Parties must list relevant documents in their

---

because, once the documents were in ATO's possession, they could be used under the statutory powers granted by the Income Tax Assessment Act of 1936. The court further discussed the possibility of other relief and stated that the only judicial basis for relief regarding the use of the privileged material was in equity, for breach of confidentiality.

171. *See Mobil Oil Australia Ltd. v Guina Developments Pty. Ltd*. [1983] 2 VR 34, 39–40 (Austl).

172. *See* Michael Schoenberg, 'Evidence Gathering, Confidentiality, and the Courts' (2004) 99 *AMPLA Yearbook* 114 (2004), *available at* http://www.austlii.edu.au/au/journals/AUMPLawAYbk/2004/6.pdf.

173. *See* Hamish Austin, ''Protection of confidential information in litigation'' (2003) 77(1-2) LIJ *Law Institute Victoria* 46; Schoenberg, *supra* note 171, at 114; Graeme Slattery and James Fielding, *Protecting Commercially Sensitive Documents in Litigation*, SQUIRE PATTON BOGGS (2014), *available at* https://www.squirepattonboggs.com/~/media/files/insights/publications/2014/09/protecting-commercially-sensitive-documents-in-l__/files/protectingcommerciallysensitivedocumentsinlitiga__/fileattachment/protectingcommerciallysensitivedocumentsinlitiga__.pdf.

possession, control, or power. Privileged documents are generally required to be listed in a special section of the list of documents. They are to be described in a manner that protects the privileged content but gives the opposing party and, if challenged, the court sufficient information to allow it to determine if privilege has been properly asserted. If necessary, the court can review the documents.

A party is entitled to conduct an oral examination for discovery of each opposing party. In the case of corporate entities, the opposing party is entitled to examine one—and only one—corporate representative, unless consent of the parties or leave of the court is obtained for further discovery.

There is an implied undertaking to the court not to use the disclosed information for any purpose other than the case for which the production was made.[174] Therefore, information obtained through discovery cannot be shared with parties outside the litigation and cannot be used in other proceedings. A party may apply to the court to be relieved of the undertaking, which will only be granted where it has been shown that the purpose of the disclosure outweighs the interests of privacy and the efficient conduct of civil litigation."[175]

Protective or confidentiality orders can still be made to protect highly sensitive information such as trade secrets. These orders often restrict duplication of the documents and who has access to them, both within a law firm and with respect to the client.

The Supreme Court of Canada has classified privilege into two categories—class privilege and case-by-case privilege. Class privileges include solicitor-client privilege (or legal-

174. Juman v. Doucette, [2008] S.C.C. 8; Lac d'Amiante du Québec Ltée v. 2858-0702 Québec Inc., [2001] S.C.C. 51.

175. *Juman,* [2008] S.C.C. 8.

advice privilege), litigation privilege, and settlement privilege. It also includes informer privilege, but, as that arises in the criminal law context, it is beyond the scope of this *Commentary*. Once a communication has been shown to fall within one of the classes, it is presumed to be nondisclosable.[176]

Case-by-case privilege depends on each specific case, and the court must perform a balancing analysis to determine whether a specific communication is privileged by applying the four-part *Wigmore* test.[177]

Where non-parties share a common interest, the disclosure of privileged documents between them does not waive the privilege. This most often applies to experts but can go beyond that. The common interest can be in a litigation matter or in the obtaining of legal advice.[178]

Solicitor-client privilege (or legal-advice privilege) applies to communications between a lawyer and a client for the purpose of giving legal advice. It is based on the recognition that the justice system depends on full, frank, and free communication between those who seek legal advice and those who provide it. The privilege belongs to the client, not the lawyer. Thus, the lawyer must not disclose privileged information without the consent of the client.

Solicitor-client privilege was originally a rule of evidence, protecting communications only to the extent that a solicitor could not be forced to testify about communications with a client. It has since evolved into a substantive legal rule, meaning

176. Lizotte v. Aviva Ins. Co. of Can., [2016] S.C.C. 52.

177. M. (A.) v. Ryan [1997] 1 S.C.R. 157.

178. Fraser Milner Casgrain LLP v. Minister of National Revenue, [2002] B.C.S.C. 1344; Iggillis Holdings Inc. v. Canada (National Revenue) [2018] F.C.A. 51.

that it extends beyond a rule of admissibility, protecting client confidences in any context.[179]

Solicitor-client privilege falls just short of being absolute. It is to be abrogated only on the basis of necessity, for example, inspection of incoming mail at a penitentiary for the purposes of safety and security. [180]

Litigation privilege is a class privilege. It applies to information gathered or created for the dominant purpose of actual or anticipated litigation. The existence of litigation privilege does not depend on the involvement of counsel. Documents prepared by a litigant or a third party at a litigant's request are protected, as long as the "dominant purpose" test is met.[181] The privilege ends with the litigation.[182]

Settlement privilege is another class privilege.[183] Settlement privilege applies to all communications for the purpose of settlement. It is not necessary that a communication be marked or negotiations specifically agreed to be "without prejudice"; what matters is whether the communication was made with the intent to settle a dispute. Settlement privilege attaches not only to unsuccessful negotiations but also to successful negotiations unless the settlement agreement itself is in issue in subsequent proceedings. Exceptions may be made to settlement privilege if it can be shown that a competing public interest outweighs the

179. Smith v. Jones [1999] 1 S.C.R. 455.

180. Ontario (Ministry of Correctional Services) v. Goodis, [2006] S.C.C. 31, para. 20

181. Blank v. Canada (Dept. of Justice), [2006] S.C.C. 39; *Lizotte,* [2016] S.C.C. 52.

182. *Blank*, [2006] S.C.C. 39, para. 36

183. This and the following propositions were confirmed by the Supreme Court of Canada in *Sable Offshore Energy Inc. v. Ameron International Corp.*, [2013] S.C.C. 37.

public interest in encouraging settlement; examples include allegations of fraud or undue influence.

3. United Kingdom

In the United Kingdom, legal-advice privilege will generally protect communications between a client and lawyer if the purpose of the communication is legal advice. A lawyer must be present when privileged communications are made. To maintain the privilege, the lawyer may only give advice to an "authorized" client. An authorized client is an individual who is explicitly approved to request and receive legal advice, for example, on behalf of a business.[184] Documents that reflect such privileged legal communications may also be privileged, for example, if forwarded to another authorized client. However, the legal-advice privilege is not absolute, and courts may make clear distinctions between legal and business advice; the latter is not covered by the legal-advice privilege.[185] Litigation privilege is also recognized in the United Kingdom and protects communications and documents created once litigation is anticipated or has begun if their main purpose is for use in that litigation.

In the United Kingdom, the Civil Procedure Rules and Practice Directions[186] govern the disclosure of documents in adversarial proceedings. Disclosure rules generally require that

184. RBS Rights Issue Litigation [2016] EWHC (Ch) 3161. Legal advice privilege attaches between lawyer and client individuals authorized to obtain legal advice on behalf of the client. In this case, privilege was denied over lawyer interview notes with employees not authorized by the client to obtain legal advice.

185. Kerman v. Akhmedova [2018] EWCA (Civ) 307. Lawyer cannot rely on client legal privilege to avoid giving evidence about a client's assets.

186. *Available at* https://www.justice.gov.uk/courts/procedure-rules/civil/rules.

litigants collect and review potentially relevant documents and then state to the other parties whether disclosable documents exist (or have existed). Disclosure may occur in a variety of avenues, but the most common is the standard disclosure. Standard disclosure requires parties to disclose documents on which they rely, documents that adversely affect their case or another party's case, documents that support another party's case, and documents that the party is required to disclose by a relevant Practice Direction.[187]

In standard disclosure, disclosed documents are served to other parties in a "list."[188] Following disclosure, other parties generally have a right to copy the disclosed documents during a process known as "inspection."[189] In making a disclosure under the standard-disclosure process, a party's list must indicate those documents to which a party claims a right or duty to withhold inspection.[190] A party may withhold inspection of documents that the party claims are privileged under the legal-advice privilege, the litigation privilege, or other privileges and confidentiality or secrecy obligations.[191] However, claiming one of these privileges may not allow a party to avoid including the potentially privileged documents in the party's list.[192] Instead, a person must apply for an order to withhold disclosure of a document.[193]

The civil procedure rules typically limit parties' use of disclosed documents to purposes related to the proceeding in

187. U.K. Civil Procedure Rules (CPR) 31.6.

188. CPR 31.10(2).

189. CPR 31.15.

190. CPR 31.10(4).

191. CPR 31.19(3).

192. *Id*.

193. *Id*.

which they were disclosed.[194] The court may also, on application of a party to the proceedings or the document's owner, order the restriction or prohibition of the use of a disclosed document.[195] Despite the protections that the Civil Procedure Rules afford, some litigants seek additional protection through the use of confidentiality "rings" or "clubs," which are analogous to the "confidentiality" and "attorneys' eyes only" designations made in American courts. Confidentiality rings limit the inspection of documents to limited categories of individuals and may be used to protect highly confidential information, such as trade secrets. However, in a recent case governing the propriety of confidentiality rings, the High Court explained that confidentiality rings are exceptional, must be limited to the narrowest extent possible, and require careful scrutiny by the Court to ensure that they do not promote unfairness.[196]

4. United States[197]

The United States permits expansive pretrial disclosure of information relevant and proportionate to a matter's claims and defenses. The philosophy of full pretrial disclosure was put in place in 1938 through the adoption of the Federal Rules of Civil

194. CPR 31.22.

195. *Id*.

196. Infederation Ltd. v. Google LLC, [2020] EWHC 657 (Ch).

197. Additional information on privilege in the United States can be found in a number of places throughout this *Commentary*. We also recommend Jenner & Block's regularly updated guide, *Protecting Confidential Legal Information: A Handbook for Analyzing Issues Under The Attorney-Client Privilege And The Work Product Doctrine*, edited by David M. Greenwald and Michele L. Slachetka, *available at* https://jenner.com/system/assets/publications/19060/original/2019%20Jenner%20&%20Block%20Attorney-Client%20Privilege%20Handbook%20(Final)%20WEB.pdf?1561056973.

Procedure.[198] All states have followed suit, and the philosophy is embedded in procedural rules in the United States. Few other countries require the extent of disclosure that the U.S. pretrial procedures require. Consequently, litigants, courts, and government agencies in other countries may be unaccustomed to the myriad jurisdictions' practices and expectations regarding disclosure, privileges, and other protections from disclosure.

The attorney-client privilege is one of the oldest privileges protecting confidential communications.[199] The Supreme Court of the United States has stated that by assuring confidentiality, the privilege encourages clients to make "full and frank" disclosures to their counsel, who are then better able to provide candid advice and effective representation.[200] The source of the attorney-client privilege in the U.S. is the ethical rules established by each of the state bar associations governing attorney practice obligations in each state, as well as the American Bar Association (ABA) Model Rule 1.6 on Confidentiality of Information, upon which most states' rules are based: "A lawyer shall not

198. The Federal Rules of Civil Procedure govern the scope of discovery in federal courts, and similar state civil procedure rules govern the scope of discovery in state courts. In general, parties may obtain information from opposing parties or third parties that is relevant to a claim or defense in the adversary proceeding. FED. R. CIV. P. 26(a). The scope of discovery is broad, and courts typically interpret the "relevance" concept liberally.

Discovery, however, has limitations. Parties may not obtain documents and information where the costs associated with procuring that information are disproportionate to the discovery needs of the case. FED. R. CIV. P. 26. Parties believing that an opposing party's discovery is harassing, duplicative, or seeks proprietary information may seek a protective order that either limits disclosure to the parties in the case, certain personnel of corporate parties, or to the party's attorneys. FED. R. CIV. P. 26(c). Parties may not obtain information protected by an evidentiary privilege or other substantive protective doctrine.

199. Swidler & Berlin v. United States, 524 U.S. 399, 403 (1998)

200. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b)." The attorney-client privilege doctrine is further refined by numerous state and federal court decisions.

Under U.S. law, the attorney-client privilege applies only to communications related to legal advice and does not apply to nonlegal business advice or opinions. The privilege will not protect communications between attorney and client made in the furtherance of a crime or fraud. Generally, to receive the protection of the attorney-client privilege in the United States, it is necessary to show, among other things, *that the communication was intended to be and was in fact kept confidential*.[201] The attorney-client privilege may be waived through voluntary, intentional disclosure of confidential communication to someone outside the attorney-client relationship. The privilege can also be waived through inadvertent disclosure, such as by producing an otherwise privileged document or by having a confidential conversation in an area where a third party overheard it. Further, if a communication is made accessible to in-house counsel in a country that does not recognize the privilege or does not recognize the privilege for in-house counsel, a U.S. court could find the attorney-client privilege has been waived based on the rationale that there was no intent to keep the information confidential, as evidenced by the fact that it was communicated to the foreign in-house counsel.[202]

---

201. *See* United States v. Mejia, 655 F.3d 126, 132 (2d Cir. 2011).

202. *See, e.g.,* Astra Aktiebolag v. Andraz Pharm., Inc., 208 F.R.D. 92 (S.D.N.Y. 2002) (applying multiple foreign laws: German law to certain communications; Korean law to others; and United States law in other circumstances depending on the law of the country with the predominant interest); Baxter Int'l, Inc. v. Becton, Dickinson and Co., No. 17-C-7576, 2019 WL

In cases of inadvertent disclosure, the inquiry may include the level of care in maintaining confidentiality, the amount of time that elapsed before the disclosure was discovered, and the significance of the disclosure. Accordingly, counsel should set up a defensible privilege review protocol and act immediately to retrieve any inadvertently disclosed privileged documents or information to avoid waiver. Although rare, disclosure may trigger "subject matter waiver" where "fairness requires a further disclosure of related, protected information, in order to prevent a selective and misleading presentation of evidence to the disadvantage of the adversary."[203]

The work-product doctrine, by contrast, is a procedural rule that protects from discovery documents that are created by a party or its attorney in anticipation of litigation. Although a party may overcome a work-product assertion upon proving a

---

6258490 (N.D. Ill. Nov. 22, 2019) (finding a waiver of privilege when privileged documents were not carefully guarded but rather injected into the case); Gucci Am., Inc. v. Guess?, 271 F.R.D. 58 (S.D.N.Y. 2010) (applying the "touch base" approach for determining which country's law applies to claims of privilege involving foreign documents and noting that communications relating to proceedings in the United States or reflecting the provision of American legal advice will be found to touch base with the United States); Smithkline Beecham Corp. v. Apotex Corp., 193 F.R.D. 530 (N.D. Ill. 2000) (holding that the party seeking to withhold the materials bears the burden of establishing the privilege, including providing the court with the applicable foreign law and demonstrating that the privilege applies to the documents it seeks to exclude from discovery); Teradata Corp. v. SAP SE, No. 18-cv-03670-WHO, 2019 WL 5698057 (N.D. Cal. Nov. 4, 2019) (reviewing choice-of-law considerations and applying the "touch base" approach to find United States privilege laws applied); Veleron Holdings, B.V. v. BNP Paribas SA, No. 12-CV-5966, 2014 WL 4184806 (S.D.N.Y. Aug. 22, 2014) (applying the "touch base" test in accordance with the Second Circuit's choice-of-law analysis and noting that the jurisdiction with predominant interests is that where the allegedly privileged relationship was entered into or where the relationship was centered when the communication was sent).

203. FED. R. EVID. 502 advisory committee's note.

requisite level of need, the doctrine generally prohibits a party or its attorney from disclosing litigation strategies, legal opinions, and related deliberations.[204]

U.S. common law also recognizes the joint-defense privilege and common-interest doctrine, which are all effectively methods for avoiding a privilege waiver when communicating with certain third parties with a shared interest in the litigation or other shared interests. Although separate and distinct, the joint-defense privilege and common-interest doctrine are often treated as one privilege.[205]

As a strictly legal matter, the joint-defense privilege is a misnomer, because it is not actually an affirmative privilege; rather, it is an exception to the rule on waiver. Generally, sharing privileged and confidential information with a third party constitutes a waiver of the privilege. However, those protected by a joint-defense agreement can avoid a waiver and preserve the privilege notwithstanding the sharing of confidential information with third parties who are part of the agreement. Arising out of joint-defense agreements in the context of criminal representation, the privilege has evolved to include any parties whose positions in a case or transaction are so aligned that they all equally benefit from the same outcome. The privilege covers communications among lawyers representing different clients who share a common legal interest. Any communications between the lawyers and between any specific client representative and any lawyer on the team are privileged based on the

204. FED. R. CIV. P. 26(a). The common-interest doctrine is not an evidentiary privilege but rather a nonwaiver doctrine. This doctrine permits parties represented by separate counsel but with a common legal interest to share previously protected information without waiving those protections.

205. The joint-defense privilege is narrower than the common-interest doctrine and arises from actual litigation, while the common-interest doctrine does not require litigation to be pending.

common interest shared by all. Communications among client representatives without counsel present, however, would not be covered by privilege. This is because the privilege still involves the need to communicate with counsel, and the subject of the communication must be legal advice that affects all the parties. Discussions between parties are thus not generally included.[206]

The common-interest doctrine applies to parties who have aligned legal positions that are all implicated in the matter.[207] Therefore, it may be possible for in-house counsel representing different legal entities within a corporate family to consider sharing defensive strategies based on this doctrine if each entity is a party (or potential party) to the same or an identical lawsuit or legal matter. Due to the rather technical nature of the common-interest doctrine and joint-defense privileges, it is important that any decision to proceed on this basis be documented among the relevant parties. Although this documentation is not strictly required, it is frequently helpful in demonstrating the common-interest or joint-defense privilege in related discovery disputes.

---

206. *See generally* discussion of common-interest privilege in *In re Teleglobe Communications Corp.*, 493 F.3d 345 (3d Cir. 2007).

207. Duplan Corp. v. Deering Milliken, Inc., 397 F. Supp. 1146, 1172 (D.S.C. 1974). *See also* FED. R. CIV. P. 26(a). The common-interest doctrine is not an evidentiary privilege but rather a nonwaiver doctrine. This doctrine permits parties represented by separate counsel but with a common legal interest to share previously protected information without waiving those protections. *In re Teleglobe Commc'ns Corp.*, 493 F.3d at 345. The scope of this nonwaiver doctrine lacks uniformity across federal and state jurisdictions, but generally the doctrine applies when the parties have a common legal, as opposed to a common business or commercial, interest regarding anticipated or pending litigation. Under this doctrine, the attorneys for the parties sharing the common legal interest may share privileged information without waiving any protection. *Id.* at 363 n.17.

B. Civil Law Exemplar Jurisdictions

1. Belgium

The Belgian legal system has a legal professional privilege. Lawyers cannot, with a few exceptions, reveal confidential information entrusted to them in the context of representing a client. Lawyers admitted to the Bar ("*advocaten*" in Dutch, "*avocats*" in French)[208] are subject to a duty of attorney-client privilege, which is called "professional secrecy."[209]

The obligation of strict professional secrecy for lawyers in Belgium is laid down in the Belgian Bar's Code of Ethics, rules of professional conduct that lawyers are obliged to comply with. The Belgian Constitutional Court has held that the legal basis for this professional secrecy obligation is a combination of Articles 10, 11, and 22 of the Belgian Constitution as interpreted in light of Articles 6 and 8 of the European Convention on Human Rights and Articles 7 and 47 of the European Union Charter. Further, Article 458 of the Belgian Criminal Code includes a sanction for lawyers who violate professional secrecy.[210] Professional secrecy can also be considered as part of the contractual obligation between the lawyer and the client.

Professional secrecy covers oral and written information, including phone calls, email, letters, notes, legal opinions and advice, and drafts or other preparatory documents. Professional secrecy also protects the lawyer's agenda, invoices, and bank account (with respect to the identity of the clients). Under

208. Only lawyers admitted to the Bar are entitled to appear and plead in court (with a few exceptions such as trade union delegates who can represent employees (members of the trade union) before Labor courts).

209. "Beroepsgeheim" in Dutch and "secret professionnel" in French.

210. In this Section concerning Belgium, the *Commentary* does not discuss the European sources such as the articles 6 and 8 of the European Convention on Human Rights in depth.

professional secrecy obligations, lawyers are required to maintain the confidentiality of all information and documents entrusted to, heard by, or discovered by the lawyer in the context of his or her representation of the client. The source of the information is not relevant. Professional secrecy covers information received directly from the client, but also information provided to the lawyer by third parties, including the adverse party. Professional secrecy applies from the point that the lawyer receives the information and is not time limited. All correspondence between the lawyer and the client, and all advice provided by the lawyer during the representation of the client, whether of a litigation or nonlitigation nature, is also considered confidential and subject to the professional secrecy obligation.[211] However, the legal privilege does not apply to official documents and case materials such as judgments or trial briefs that are public.

There are some exceptions to the general principle of professional secrecy. Professional secrecy can, for instance, be overridden if a higher value is at stake, for example, to prevent imminent harm.[212] The lawyer's professional secrecy may also be put aside to defend the lawyer's own rights in court. The right of defense is considered to be of a higher value than the professional secrecy obligation. Also, if a lawyer commits (or participates in) a crime, professional secrecy can no longer be invoked, as the lawyer is acting outside the scope of legal representation.

Under Belgian law, contrary to some common law jurisdictions, there is no formal process of disclosure in civil law court proceedings. Parties should produce their own exhibits

211. Belgian Supreme Court, Oct. 3, 2018, case P.18.0235.F. Article 458 of the Criminal Code does not prevent the lawyer's client, the person protected by that provision, from producing, in his or her defense, his or her correspondence with the lawyer.

212. In practice, in such cases, the lawyer will inform the President of the Bar, who will then contact the Public Prosecutor.

supporting their claims or defenses. However, parties are obliged to cooperate in good faith with respect to the production of documents. The court may also require a party to produce documents that are needed to make a judgment.

Correspondence between Belgian lawyers is, in principle, confidential and cannot be used as evidence. There are some exceptions to this principle. Some correspondence between lawyers will be classified as "official" and can be produced in court. The Bar's Code of Ethics explains how the distinction between confidential and official correspondence should be drawn. Possible conflicts in this respect are resolved by the President of the Bar.

Legal actions taken in violation of the legal privilege will be deemed null and void. For example, criminal prosecutions or other regulatory investigations conducted on the basis of privileged information are not permissible except in exceptional circumstances,[213] for instance, if the legally privileged document itself constitutes a criminal offense or could establish the lawyer's participation in a criminal offense. In civil cases, the Belgian courts cannot accept privileged information as evidence.

Lawyers working as in-house counsel are not members of the Belgian Bar. Hence, they do not need to comply with the Bar's Code of Ethics, including the professional secrecy duty. However, legal advice given by "in-house counsel"[214] for the benefit of their corporate employer and within their role as legal

213. Belgian Constitutional Court, Jan. 23, 2008, case 10/2008. Information that the lawyer has obtained while carrying out the essential activities of his or her profession, such as assisting and defending a client in court and providing legal advice, even outside any legal proceedings, remains covered by professional secrecy and cannot be disclosed to the public authorities.

214. As defined by the Act of March 1st, 2003, establishing the Institute for in-house counsel.

counsel is deemed "confidential" by law.[215] The legal professional privilege for in-house counsel covers legal advice to the employer but also internal requests for legal advice, correspondence related to the advice, and preparatory notes and drafts.[216]

2. Brazil

The Brazilian Constitution recognizes lawyers as essential to the administration of justice. The conduct of attorneys and the attorney-client relationship in Brazil are regulated primarily by federal law[217] and the Code of Ethics and Discipline propounded by the Brazilian Bar Association. Other sources of authority concerning the conduct of attorneys include the Code of Civil Procedure and the Code of Criminal Procedure.[218]

Under Brazilian law, attorneys have a duty to protect the confidentiality of all information a client discloses to them, whether learned in the context of a litigation or in connection with providing other legal services.[219] Unless there are

215. *Cf.* article 5 of the Act of March 1st, 2003.

216. Brussels Appeal Court, Mar. 5, 2013. Recognition of in-house legal counsel privilege (with reference to the Act of March 1st, 2000). While this decision concerned the specific context of an investigation by the Belgian competition authorities, its effect could go beyond this context and strengthen the recognition of the in-house counsel privilege in other areas as well.

217. Estatuto da Advocacia e da Oab, Lei 8906/94 (Law No. 8906 of July 4, 1994) ("Statute") and the General Regulations of the Bar Association Statute.

218. For example, Section 297 of the Brazilian Criminal Procedural Code ("Code") exempts from the duty of giving testimony anyone who must keep privilege due to his profession. The Brazilian Civil Procedural Code has a similar provision in Section 406, II. With respect to internal investigations, practitioners should consult Provision 188/2018, which provides that attorneys have to keep all information gathered in an investigation confidential.

219. *See generally* Statute Articles 1 and 7; Code Chapters 26, 35.

exceptional circumstances, attorneys cannot disclose, and cannot be compelled to disclose, a client's confidential information. Those protections extend to all of the attorneys' files and communications and are generally inviolable. An attorney's obligation to maintain confidentiality and the associated protections afforded an attorney's files remain even after the attorney-client relationship is terminated.

Exceptional circumstances that may allow for an attorney to disclose otherwise confidential information are rare and include instances such as where there is a "severe threat to life or honor" or where disclosure is necessary for the attorney's defense.[220] Any breach of a client's confidentiality is a serious matter and can result in administrative, civil, and even criminal sanctions for an attorney if there was no good cause for the disclosure.[221]

Confidentiality obligations and protections apply to any qualified attorney, including in-house counsel. In addition, Brazil's Constitution protects professional secrecy by individuals whose duties require access to information generally considered private and confidential, which arguably includes in-house counsel. Nonetheless, some courts in Brazil have found that documents and information in the possession of in-house counsel were not protected because in-house counsel was viewed as an employee. In light of potential uncertainties concerning the protections afforded materials shared with in-house counsel, it may be prudent in particularly sensitive or contentious situations to assume communications and materials shared with Brazilian in-house counsel will not be protected. Moreover, as in many other jurisdictions, if in-house counsel provides business

220. *See generally* Code Chapter 3.

221. *E.g.*, Article 154 of the Brazilian Criminal Code (breach of professional secrecy without good cause is a crime).

advice rather than legal advice, the communication is not protected.

3. China

China has no formal discovery process and lacks general privilege rules that protect documents and information during discovery. China has no real equivalent to the attorney-client privilege or work-product protections found in other jurisdictions.

China's Lawyer's Law requires that lawyers keep clients' information confidential and protect the privacy of their clients, including state and trade secrets disclosed to the lawyer in the context of the client's representation.[222] These confidentiality and privacy obligations do not, however, extend to crimes committed by clients that could affect national or public security, which must be disclosed by the lawyer.[223]

Lawyers can be sanctioned for failing to disclose important information to a Chinese court if the court requests the information.[224] Chinese laws may also require the disclosure of confidential client information to governmental authorities. Citing China's absence of legal privilege, U.S. courts have allowed subpoenas and discovery requests for documents and information between Chinese counsel and their clients, although in practice, obtaining the documents and information may be difficult.[225]

---

222. China Lawyer's Law (2009), arts. 33 and 38.

223. *Id*.

224. China Civil Procedure Law, arts. 67 and 72.

225. *See, e.g.*, Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468 (9th Cir. 1992).

4. European Union

Legal professional privilege in the European Union flows from the fundamental rights to be advised, defended, and represented and the right of defense as enshrined in Articles 47 and 48 of the Charter of Fundamental Rights of the European Union.[226] Based on case law by the European Court of Justice, there are generally three categories of legal professional privilege recognized: (1) written communication between a party and an independent attorney barred in one of the member states (this excludes in-house counsel in most member states); (2) internal notes reflecting such communications; and (3) documents drawn up exclusively to seek legal advice from an attorney in exercising the rights of defense. These categories tend to be narrowly interpreted.

The European Union has drawn a meaningful distinction between communication with lawyers designated as *in-house counsel* and *outside counsel* in determining whether the communication is privileged.[227] In *Akzo Nobel*, the EU's Court held that lawyers employed as in-house counsel could not engage in privileged communications with their client, the corporation.[228] Under EU law, the analysis of whether a corporation's

226. F. Enrique Gonzales & Paul Stuart, *Legal Professional Privilege under EU Law: Current Issues,* COMPETITION LAW AND POLICY DEBATE, Sept. 2017, at 56, *available at* http://awa2018.concurrences.com/IMG/pdf/12._f.e._gonzalez-diaz_and_p._stuart_-_legal_professional_privilege_under_eu_law.pdf.

227. *Id.* Akzo Nobel Chems. Ltd. v. Comm'n of the European Cmtys., 2008 Bus. L.R. 348 (Ct. of First Instance 2007). *See also* C-155/79, AM&S Europe Ltd. v. Commission of the European Communities, 1982 E.C.R. 1575, holding that protected communications are those made by a lawyer licensed in a member state for the purpose of the clients' right of defense.

228. 2008 Bus. L.R. 348. The court affirmed the decision of the lower courts that the communications at issue with in-house counsel were not privileged under the rules established in C-155/79 AM&S Europe Ltd v. Commission, 1982 E.C.R. 1575.

communications with a lawyer are privileged is a two-step process.[229] First, the lawyer must be categorized as independent and cannot be bound to their client because of employment. Second, the communication between the independent lawyer and the client must involve legal advice and be made for purposes of the client's right of defense.[230] The *Akzo* court distinguished between communications with in-house counsel and outside counsel, holding that the same communication was protected from disclosure with outside counsel because they are "independent" for purposes of privilege, but that in-house counsel was not independent.[231] The *Akzo* ruling undermines the predictability of applicable privileged in those member states where in-house counsel communications have an expectation of privilege.[232]

The *Akzo* ruling had an additional impact on privilege by excluding lawyers qualified outside of the European Union from the application of legal professional privilege.[233] After the court established that privilege applies only to communication between a client and an independent lawyer, the court further limited privilege to lawyers "'entitled to practice [their] profession in one of the Member States, regardless of the Member State in which that client lives but not beyond those limits.'"[234] This *Akzo*

229. John Gergacz, *Privileged Communications with In-house Counsel under United States and European Community Law: A Proposed Re-Evaluation of the* Akzo Nobel *Decision*, 42 CREIGHTON L. REV. 323, 330–31 (2009).

230. *Akzo Nobel*, 2008 Bus. L.R. 348 at 374. The court found that in-house counsel did not constitute an "independent" lawyer and could not therefore engage in privileged communications with the corporation. *Id.* at 382–84.

231. *Id*.

232. Gergacz, *supra* note 229, at 335.

233. Justine N. Stefanelli, *The Negative Implications of EU Privilege Law under Akzo Nobel at Home and Abroad*, 60 INT'L & COMP. L.Q. 545, 545 (2011).

234. *Id.* at 546.

ruling has significant implications for cross-border business relationships. The United States and European Union, for example, have become heavily integrated through multijurisdictional business ventures and transnational companies.[235] The exclusion of non-EU attorneys from EU privileges runs the risk of complicating international business transactions and weakening the communications between clients and their counsel due to the fear of disclosure.[236] In light of the *Akzo* ruling, it is important for multinational companies and their counsel to analyze carefully the scope of privilege that governs their communications.

On 26 November 2018, the European Commission submitted a helpful overview of its policy on the treatment of legally privileged information in competition proceedings in the context of that year's Organisation for Economic Co-operation and Development roundtable discussions.[237] This policy makes it clear that the European Commission recognizes that privilege may exist and will not compel privileged documents or require parties to use them as evidence in competition proceedings. However, the European Commission may still very narrowly define the scope of the privilege that may exist.

5. France

As in many civil law jurisdictions, the French Code of Civil Procedure does not provide for general discovery like that found in common law jurisdictions. Article 9 of the Code of Civil Procedure provides that "[e]ach party must prove,

235. *Id.* at 556.

236. *Id*.

237. The European Commission submission to the Organisation for Economic Co-Operation and Development is available at https://one.oecd.org/document/DAF/COMP/WP3/WD(2018)46/en/pdf.

according to the law, the facts necessary for the success of his claim."[238] Generally, parties must only disclose the evidence supporting their factual and legal arguments "in due time," which is generally understood to be when the party relies upon the evidence in a proceeding before the judge.[239] Yet, the judge also has the power to order "any legally appropriate investigation measures," and each party may petition the judge to ask the other side, or third parties, to produce evidence.[240] The decision whether a party should produce the requested evidence is at the judge's discretion. Judges order production where "there is a legitimate reason to preserve or establish" the evidence or when the party pleading the fact "does not have sufficient material to prove it."[241] Otherwise, there is no general obligation to disclose documents or evidence prior to trial or to preserve any such evidence.

Because of the narrow discovery allowed under the Code of Civil Procedure, French law has not fully developed an attorney-client privilege concept. French attorneys are bound not to disclose documents or evidence under either the French Criminal Code or the National Rules of the French Bar Council (*Réglement Intérieur National*). Under Article 2 of the National Rules, professional secrecy exists to protect communications between attorneys, or *avocats*, and their clients, regardless of the medium or context of such discussions.[242] As such, this professional obligation of secrecy applies to cover legal opinions provided to clients, correspondence between the attorney and client, notes

238. CODE CIVIL [C. CIV.] [CIVIL CODE] art. 9 (Fr.).

239. *Id.*, art. 15.

240. *Id.*, arts. 10, 11.

241. *Id.*, arts. 145, 146.

242. Réglement Intérieur National [National Rules of the French Bar Council], art. 2.

taken by the attorney, information and documents provided to the attorney, the payment of fees by the client, and even extends to protect information required by French auditors.[243] French law provides that documents falling under the professional obligation of secrecy may not be used as evidence during civil litigation.[244] However, France does not recognize the same protections for in-house counsel (*juristes d'entreprise*), who are treated as a separate professional track from *avocats*.[245]

Due to the limited circumstances in which documents may be discovered under the Code of Civil Procedure, there are restrictions on which documents may be designated as "confidential" and kept from public disclosure. French Decree No. 2018-1126, creating Commercial Code Articles R. 153-1 to R. 153-9, allows judges to order that documents seized are to be treated as confidential.[246] The Decree also creates a procedure by which litigants may seek judicial intervention to protect the confidentiality of such documents.[247]

---

243. *Id*.

244. Loi 71-1130 du 31 décembre 1971 portant réforme de certaines professions judiciaires et juridiques [Law 71-1130 of 31 December 1971 on the reform of certain judicial and legal professions], art. 66.5, JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL JOURNAL OF THE FRENCH REPUBLIC].

245. DLA PIPER, LEGAL PRIVILEGE GLOBAL GUIDE 53–55 (June 1, 2020), *available at* https://www.dlapiperintelligence.com/legalprivilege/insight/handbook.pdf.

246. Ozan Akyurek, Thomas Bouvet, Bénédicte Graulle & Cyril Philbert, *New French Decree Strengthens Protection of Confidential Documents*, JONES DAY (Feb. 5, 2019), https://www.jdsupra.com/legalnews/new-french-decree-strengthens-98206/.

247. *Id*.

6. Germany

German law does not recognize legal privilege as an overall concept as is routine in common law jurisdictions. Attorney-client communication and attorney work product are therefore not protected as such. Germany instead imposes a professional secrecy obligation on lawyers (*Rechtsanwalts*) that prohibits them from disclosing client-related information that comes into their possession.[248] This secrecy obligation is the functional equivalent of a legal professional privilege but does not often arise because of Germany's limited discovery obligations. The professional secrecy obligation does not apply to in-house attorneys, so they may not invoke the obligation to avoid court-ordered production of documents, especially in criminal proceedings.

Attorneys have a right to refuse testimony,[249] including the right to refuse the production of documents in their possession, but this right does not attach to the document itself. For example, a document is not protected if it is in the possession of the client. Pretrial discovery is not inherent in the German system. Each party must instead obtain and produce the facts and evidence relevant to its argument directly, without cooperation of the opposing party (with limited exceptions, for example, in cartel follow-on damages cases). Exceptionally, the court may order a party to produce specific documents (to the court, not to the opponent), but this instrument is rarely used in practice.[250] If ordered by the court, a party cannot refuse the production of such documents even if they contain attorney-client

248. Bundesrechtsanwaltsordnung [The Federal Lawyers Act], 1994, § 43a(2).

249. ZIVILPROZESSORDNUNG [ZPO] [CODE OF CIVIL PROCEDURE] § 383(1)(6).

250. Section 142 of the German Code of Civil Procedure provides that "The court may direct one of the parties or a third party to produce records or documents, as well as any other material, that are in its possession and to which one of the parties has made reference."

communication or attorney work product, although in ordering the production of documents, the court should consider whether the documents could contain any confidential information. Lawyers can refuse the production of such documents based on their right to refuse testimony. This applies to outside counsel only and only those outside counsel enrolled at the German Bar or those recognized as equivalent (generally lawyers from other EU jurisdictions). In-house counsel do not have the right to refuse testimony and accordingly no right to refuse production of documents.

The German legal system does not have formal discovery procedures, and pretrial discovery in Germany is nonexistent.[251] German courts supervise adversary proceedings and typically request that each party presents all relevant evidence. These courts also issue orders for the taking of evidence that specify which evidence parties should obtain to establish a particular fact.[252] Each party bears the burden of proving the facts on which it bases a claim or defense. The parties decide which facts and documents to submit to the court in support of a claim or defense but have no obligation to disclose all information, even if it is relevant to the case.[253] However, there is a general obligation that the parties cannot mislead the court. A party may ask the court to compel the production of a document if the

251. *Privilege and disclosure*, GLOBAL LEGAL INSIGHTS, https://www.globallegalinsights.com/practice-areas/litigation-and-dispute-resolution-laws-and-regulations/germany#chaptercontent3. (last visited July 13, 2022).

252. *Id*.

253. Stefan Rutzel, Andrea Leufgen & Eric Wagner, *Litigation and enforcement in Germany: overview*, GLEISS LUTZ, https://content.next.westlaw.com/Document/I2ef128401ed511e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true (last visited July 13, 2022).

document is known to be held by the other party—for example, if the opposing party has referred to the document on the record.[254]

Although there is a specific and narrow prohibition against the seizure of communications between attorneys and clients in the context of criminal investigations,[255] Germany's highest judicial body, the Federal Constitutional Court, ruled in 2018 that prosecutors who raided law offices of Volkswagen's outside counsel in Munich could proceed in reviewing the seized materials.[256] Volkswagen had retained outside counsel to conduct an internal investigation into the company's 2015 emissions testing protocols. The investigation covered activities at Volkswagen and Audi, a subsidiary of Volkswagen, but Audi had not formally entered into a relationship with the law firm. In relation to a criminal investigation into Audi, German prosecutors raided outside counsel's offices in Munich and seized documents. Outside counsel and Volkswagen filed suit to prevent prosecutors from reviewing the documents and other information related to the internal investigation. The German Federal Constitutional Court rejected their bid to block review, ruling that under German law, the materials were not covered by attorney-client privilege, as no such direct relationship existed between Audi and the outside counsel. In this decision, German courts highlighted the requirement of a direct relationship between attorney and client to invoke attorney-client privileges and ruled that the privilege does not extend to subsidiaries or

254. ZIVILPROZESSORDNUNG [ZPO] [CODE OF CIVIL PROCEDURE] § 421 et seq.

255. This right is protected by Article 6(3) of the European Convention on Human Rights and Articles 2(1) and 20(3) of the German Constitution, which protect the right of an effective defense, but this is limited to defense work product.

256. BVerfG [Federal Constitutional Court], 2 BvR 1405/17, 2 BvR 1780/17, 2 BvR 1562/17, 2 BvR 1287/17, 2 BvR 1583/17, June 27, 2018.

affiliates, unless they too enter into a separate, formal relationship with outside counsel.

7. Japan

As a civil law country, Japan's litigation and evidence-gathering concepts operate quite differently than in its common law counterparts.[257] Though Japan, like the United States, has a Code of Civil Procedure (*Minji Soshōhō*), "the scope of discovery in Japan is far narrower than that in the United States, and Japan does not have the same type of pretrial discovery as the United States."[258] The Japanese judicial system views evidence gathering as a goal of *trial*, rather than a *pretrial* function, and therefore the judge plays a central role in gathering and evaluating evidence.[259] There are no depositions, and under the *Minji Soshōhō*, judges may "examine evidence on their own motion and . . . . . cross-examine parties or witnesses on their own authority."[260]

The *Bengoshi Ho* ("Lawyers Law") is an ethical code that applies to all Japanese lawyers (*bengoshi*), and it requires them to maintain the confidentiality of all information gathered in the course of their representation.[261] Importantly, though, the privilege only protects communications in the possession of *bengoshi*. If the document has been prepared by a *bengoshi* but is in

257. *See* Craig P. Wagnild, *Civil Law Discovery in Japan: A Comparison of Japanese and U.S. Methods of Evidence Collection in Civil Litigation*, 3 ASIAN-PAC. L. & POL'Y J. 1, 16 (2002).

258. Masamichi Yamamoto, *How Can Japanese Corporations Protect Confidential Information in U.S. Courts? Recognition of the Attorney-Client Privilege for Japanese Non-Bengoshi in-House Lawyers in the Development of a New Legal System*, 40 VAND. J. TRANSNAT'L L. 503, 506 (2007).

259. *Id*. at 513; Wagnild, *supra* note 257, at 4.

260. Wagnild, *supra* note 257, at 4 (citing, *e.g.*, MINSOHŌ (C. CIV. PRO.) art. 207).

261. *Id*. at 514.

the client's possession, it is not protected.[262] Further, because in-house lawyers are not considered *bengoshi*, the privilege does not currently protect "communications between a corporation and non-*bengoshi* in-house lawyers."[263]

Formal confidentiality protections are also somewhat narrower in Japan, though they do exist. Lawyers must maintain the confidentiality of information learned in performing their legal work with clients that a client would reasonably expect to be kept confidential.[264] This obligation remains after the completion or transfer of a client's matter and may extend to third parties if the information is learned by an attorney in the scope of a client's representation. Both in-house and outside counsel are subject to these confidentiality obligations. If a lawyer fails to maintain this confidentiality, the lawyer can be sanctioned under the Japan Federation of Bar Association's Code of Attorney Ethics. Disclosure of confidential information is also a criminal violation under Japanese law.[265]

As in the United States, Japan favors open court proceedings.[266] In the original version of the *Minji Soshōhō*, "the principle of open judicial proceedings was applied to trade secrets with few, if any, exceptions," but subsequent amendments have adopted protections for trade secrets, in part to ensure that

262. Joseph Pratt, *The Parameters of the Attorney-Client Privilege for in-House Counsel at the International Level: Protecting the Company's Confidential Information*, 20 NW. J. INT'L L. & BUS. 145, 161 (1999).

263. Yamamoto, *supra* note 258, at 515.

264. Bengoshihō [Attorney Act], Law No. 205 of 1949, art. 23.

265. KEIHŌ [PEN. C.], Law No. 45 of 1907. Violations may result in up to six months of imprisonment or a fine.

266. *See* ELIZABETH A. ROWE & SHARON K. SANDEEN, TRADE SECRECY AND INTERNATIONAL TRANSACTIONS: LAW AND PRACTICE 246 (2015).

Japan can remain "globally competitive."[267] Thus, the *Minji Soshōhō* contains provisions for maintaining the confidentiality of documents.[268] Lawyers may refuse court orders requiring the disclosure of client information or other confidential information in the lawyer's possession. However, if the client waives the confidentiality, the lawyer may no longer assert the refusal right.[269] The lawyer may still refuse to testify regarding such matters. These rights extend to criminal investigations but not investigations by the antitrust authority, which are considered administrative procedures by the Japanese government.

In the intellectual property context, protective orders are authorized by legislation translated literally as "Confidentiality Preservation Order under Patent Act."[270] However, "protective orders have been granted by courts in a very limited number of instances," likely because of the associated "threat of severe criminal penalties" for violating such orders.[271] Parties more commonly enter into "voluntary nondisclosure agreements."[272]

8. Switzerland

Switzerland's legal professional privilege is based on the Federal Constitution of the Swiss Confederation, the Swiss

267. *Id*. RUTH TAPLIN, INTELLECTUAL PROPERTY AND THE NEW GLOBAL JAPANESE ECONOMY 61 (2009).

268. *See* MINSOHŌ (C. CIV. PRO.) art. 92 (Restriction on Inspection, etc. for Secrecy Protection).

269. Minji Soshōhō [Civil Procedure Act], Law No. 109 of 1996, arts. 197 and 220.4(iii)).

270. Takanori Abe & Li-Jung Hwang, *Protective Order in Japan, Waves from U.S., towards Taiwan* (Dec. 2, 2010), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2257959.

271. Kyle Pietari, *An Overview and Comparison of U.S. and Japanese Patent Litigation, Part II*, 98 J. PAT. & TRADEMARK OFF. SOC'Y 970, 981 (2016).

272. *Id*.

Criminal Code, and other laws and codes binding attorneys. The Swiss Federal Constitution lays out the right to certain private life protections and the protection of personal liberty, which are the foundations for Swiss legal professional privilege.[273] Noncompliance with legal professional privilege is covered by the Swiss Criminal Code, which makes an attorney's disclosure of a secret a criminal offense with a penalty of a fine or up to three years in prison.[274] Legal professional rules bind attorneys to maintain the confidentiality of client matters and certain allegiances to clients if a contractual agreement is entered into. Swiss law does not distinguish between legal advice and litigation privileges, and privileges do not typically extend to in-house counsel's communications with employees or clients of the organization.[275] Privilege does apply to communications between in-house and outside counsel.

As long as the attorney is acting in a legal capacity, then legal professional privilege is likely to apply. Regular legal activities, including representing clients in court and before authorities and providing legal advice, are typically covered by the Swiss legal professional privilege. Even a client's identity may be considered privileged in some circumstances. Additionally, information available from a nonprivileged source can be considered privileged if the client wants the information kept secret. Corporate or other business-related types of advice, however, may

273. BUNDESVERFASSUNG [BV] [FEDERAL CONSTITUTION OF THE SWISS CONFEDERATION], arts. 10 and 13.

274. SCHWEIZERISCHES STRAFGESETZBUCH [StGB] [CRIMINAL CODE] Dec. 21, 1937, art. 321.

275. Bundesgericht [BGer] [Federal Supreme Court] Mar. 14, 2008, BE.2007.10-13, and Oct. 28, 2008, 1B_101/2008. In-house counsel may be protected by privilege if they are the only person to receive documents or information provided to the in-house counsel by the organization, and the in-house counsel is the only person allowed to transfer the documents or information.

not be covered by the privilege even when provided by an attorney, as they are not strictly legal activities.[276]

The line drawn by Swiss courts regarding legal and nonlegal activities in terms of privilege is quite nuanced. Certain other activities may themselves have mandatory disclosure requirements. For example, if a Swiss attorney also offers financial services or advice not covered by the legal professional privilege, the attorney may be obligated to report money laundering suspicions.

There are several justifications that can remove the legal professional privilege protection from documents. Among these are by the agreement of the client whose information is protected, by authorization of the Lawyers' Supervisory Authority, in situations where self-defense is required, and when the production of the information is absolutely necessary (for example, to avoid imminent danger to an individual).

According to the Swiss Private International Law Act, parties to a contract may determine which law will apply to a contract, although Swiss attorneys tend to prefer that Swiss laws apply to contracts.

C. Other Exemplar Jurisdictions

1. India—Civil and Common Law

In India, professional communication between a legal adviser and a client is accorded protection under the Indian Evidence Act 1872, the Advocates Act 1961, and the Bar Council of India Rules. Sections 126 to 129 of the Indian Evidence Act codify the common law principles on professional communications between attorneys and clients in the context of the attorney-

276. *See* Bundesgericht [BGer] [Federal Supreme Court], 1B_85/2016 and 1B_437/2017.

client relationship. These sections restrict attorneys from disclosing communications exchanged with clients; extend this protection to those working with or for the attorney; prohibit an attorney from breaking the privilege unless called upon by a client as a witness; and state that courts cannot compel the production of privileged information. For the privilege to apply, the communications must remain confidential.[277] The Bar Council of India Rules reinforce this confidentiality as part of expected professional conduct.[278] These privilege protections apply to clients only and not legal professional advisers (a term that does not clearly include in-house lawyers). India also recognizes the privilege of documents created in anticipation of litigation as legal professional privilege.[279]

The protections for in-house counsel remain open to uncertainties, due to the fact that many of the provisions in Indian law are framed with reference to an "advocate," who is someone actually practicing law before an Indian court. Rule 49 of the Bar Council of India Rules states that an advocate shall not be a full-time salaried employee of any person, government, firm, corporation, or concern.[280] If an advocate takes up such employment, they are to disclose this fact to the Bar Council and shall then cease to practice as an advocate so long as the employment continues. According to the Advocates Act of 1961, persons working in the law department of a national or multinational firm are

277. Memon Hajee Haroon Mohomed v. Abdul Karim, (1878) 3 Bom. 91.

278. *See* Bar Council of India Rules, Part VI, Chapter II, Section II, Rule 17 (attorneys cannot breach the obligations of the attorney-client relationship established in Section 126 of the Indian Evidence Act).

279. *See* Larsen & Toubro Ltd v. Prime Displays Ltd, Abiz Business (P) Ltd. And Everest Media Ltd, (2002)(5) BomCR 158.

280. *See also* Satish Kumar Sharma v. Bar Council of Himachal Pradesh, AIR 2001 SC 509 (a full-time employee is not necessarily advocating on behalf of the employer).

not recognized as lawyers and, therefore, do not enjoy the same privileges as those working in private practice. This is because they are full-time, salaried employees and thus would not be able to claim any privilege nor could any privilege be claimed on their behalf by their employers.[281] However, the same duty of confidentiality binds both in-house and outside counsel, and communications may be confidential but not privileged.

281. *See* Municipal Corp. of Greater Bombay v. Vijay Metal Works, AIR 1982 Bombay 6 (a salaried employee who advises an employer on legal questions and matters may be protected the same as barristers, attorneys, and the like).

Moving the Law Forward in a Reasoned & Just Way