The Sedona Conference Journal®

Volume 24 ❖ 2023 ❖ Number One

Articles

The Sedona Conference®

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

The Sedona Conference Journal®

Volume 24

■

2023

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 "24 Sedona Conf. J. _____ (2023)."

Publisher's Note

Welcome to Volume 24, 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 24, Number 1, of the Journal contains two nonpartisan consensus commentaries from The Sedona Conference Working Group on Electronic Document Retention and Production (WG1), two nonpartisan consensus commentaries from the Working Group on Trade Secrets (WG12), one nonpartisan consensus commentary from the Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6), and one nonpartisan consensus commentary from the Working Group on Patent Litigation Best Practices (WG10). 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 2023

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

The Hon. Hildy Bowbeer (ret.), St. Paul, MN

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

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

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

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

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

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

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

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

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. 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, Senior 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, 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 TAR CASE LAW PRIMER, SECOND EDITION

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

Author:

The Sedona Conference

Drafting Team Leaders:

Tara S. Emory — Maria Salacuse

Drafting Team:

Gareth Evans — Alicia Hawley
Emily Jennings — Robert Keeling
Leeanne S. Mancari — Angelica Ornelas
John Pappas, Jr. — Florence Yee

Steering Committee Liaisons:

Rebekah Bailey — Andrea D'Ambra
Philip Favro — Hon. Andrew J. Peck (ret.)

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, *TAR Case Law Primer, Second Edition*, 24 SEDONA CONF. J. 1 (2023).

PREFACE

Welcome to the final, May 2023 version of *The Sedona Conference TAR Case Law Primer, Second Edition*, 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.

The first edition of the *TAR Case Law Primer* was published in January 2017 to address case law issues that arose during the early use of technology-assisted review (TAR) for the exploration and classification of large document collections in civil litigation. Since publication of the first edition, case law has addressed more complex issues such as TAR methodologies, metrics, and validation. This second edition reflects the subsequent history and development of TAR case law, analyzes the published judicial decisions in the years following the original publication, and discusses how the technological shift from TAR 1.0 systems to TAR 2.0, continuous active learning, has impacted the case law. Like the first edition, the *Primer* does not recommend best practices or otherwise comment on the utility of TAR. It is intended to assist courts and practitioners in staying abreast of this evolving area of law and technology.

The *Primer* was a topic of dialogue at the WG1 2022 Midyear Meeting in Phoenix, and drafts of the *Primer* were circulated for member comment at the Midyear Meeting and again in the fall of 2022. Future developments in the law and technology may warrant further updates.

The Sedona Conference acknowledges the efforts of Drafting Team leaders Tara Emory and Maria Salacuse, who were

invaluable in driving this project forward. We also thank drafting team members Gareth Evans, Alicia Hawley, Emily Jennings, Robert Keeling, Leeanne S. Mancari, Angelica Ornelas, John Pappas, Jr. and Florence Yee, and steering committee liaisons Rebekah Bailey, Andrea D'Ambra, Philip Favro, and the Honorable Andrew J. Peck (ret.) for their dedication and contributions to this project. We also thank Deesha Shah for her assistance in compiling the Table of Cases.

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 damages and patent litigation best practices; data security and privacy liability; trade secrets; 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
May 2023

TABLE OF CONTENTS

I. INTRODUCTION

Courts have generally accepted the use of Technology Assisted Review (TAR)[1] to search for electronically stored information (ESI) responsive to requests for production. They routinely cite its benefits and encourage its use. With more frequent implementation of TAR and greater familiarity with TAR workflows, courts in recent years are handling increasingly complex TAR disputes compared with when The Sedona Conference published the first edition of the *TAR Case Law Primer* ("*First Edition Primer*") in January 2017. The *First Edition Primer* addressed the early TAR cases, providing courts and parties with authority on the common TAR issues of that time.

In the years since, case law has further developed to address more complex issues, such as TAR methodologies, metrics, and validation. This updated Primer ("*Second Edition Primer*," or "*Primer*") updates and replaces the *First Edition Primer*. This

1. TAR is "A process for prioritizing or coding a collection of electronically stored information using a computerized system that harnesses human judgments of subject-matter experts on a smaller set of documents and then extrapolates those judgments to the remaining documents in the collection. Some TAR methods use algorithms that determine how similar (or dissimilar) each of the remaining documents is to those coded as relevant (or nonrelevant) by the subject-matter experts, while other TAR methods derive systematic rules that emulate the experts' decision-making processes. TAR systems generally incorporate statistical models and/or sampling techniques to guide the process and to measure overall system effectiveness." *The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition*, 21 SEDONA CONF. J. 263 (2020) (definition adopted from Maura R. Grossman & Gordon V. Cormack, *The Grossman-Cormack Glossary of Technology-Assisted Review with Foreword by John M. Facciola, U.S. Magistrate Judge*, 7 FED. CTS. L. REV. 1, 32 (2013)). The terms "predictive coding" and "computer-assisted review" are sometimes used interchangeably with TAR to describe this process. This *Primer* will use the term "TAR," unless quoting a case that uses another term.

Primer is intended to assist courts and practitioners in staying abreast of this evolving area of law and technology. It contains all cases that substantively address TAR found by the drafting team as of December 31, 2022. It spotlights key trends and issues relating to TAR through December 31, 2022, identifies supporting case law, and summarizes the current state of the law and the open questions that remain.

The *Primer* generally addresses case law deciding disputes relating to TAR and does not address cases in which parties used TAR without challenge. Beyond the scope of the *Primer*, parties may find additional guidance on TAR uses and methodologies within stipulated TAR protocols.[2]

While it is hoped that this *Primer* will provide a thorough overview of TAR to those who read it beginning to end, it is also expected that many readers will instead focus only on topics related to specific needs. The *Primer* is therefore organized based on those topics, with some cases discussed in multiple sections.

Section II addresses the history of judicial acceptance of TAR, discussing key cases for TAR acceptance and trends and providing context for modern TAR jurisprudence. Beginning with *Da Silva Moore v. Publicis Groupe*[3] in 2012, courts began to recognize the potential value of TAR to increase efficiencies in the discovery process. As parties' use of TAR also increased and evolved, courts more recently have addressed issues relating to different TAR workflows.

---

2. In compiling the TAR case law summaries included in this *Primer*, the drafting team focused on identifying and analyzing judicial decisions related to TAR. The Primer purposefully does not summarize the terms of various TAR protocols, whether they are stipulated by the parties or "so ordered" by a court. In the drafting team's view, TAR protocols by themselves do not provide substantive guidance from judges on legal issues or disputes related to TAR.

3. Da Silva Moore v. Publicis Groupe, 287 F.R.D. 182, 183 (S.D.N.Y. 2012).

Section III discusses how courts have accepted the use of TAR when parties have agreed to its use, and how they have held parties to their prior agreements about the use of TAR. Courts, however, mostly decline to require a responding party to use TAR when it objects to doing so. In accordance with Sedona Principle 6,[4] courts generally defer to the responding party's reasonable choice of methods for collecting, reviewing, and producing its own ESI, including the use of TAR. However, courts have also acknowledged that a party's unilateral decisions about its use of TAR are subject to limitations if it is unreasonable or results in a production deficiency.

Section IV examines the level of transparency and disclosure that courts expect in connection with TAR. This section starts by discussing cases that generally address whether the use of TAR should be disclosed. It then moves on to cases about other types of disclosure—whether (and how) information about seed, training, or validation sets should be shared; whether TAR metrics and methodologies should be divulged, including during Rule 30(b)(6) depositions; and situations in which null sets and nonresponsive documents should be sampled.

Section V includes cases that address issues related to TAR workflows, including search-term culling, recall thresholds, ESI orders, and TAR protocols.

Section VI discusses how courts have considered the existence of court-ordered ESI protocols when assessing a responding party's production decisions.

The final four sections of this *Primer* examine the application of proportionality in connection with TAR (Section VII);

4. The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, Principle 6, 19 SEDONA CONF. J. 1, 118 (2018) [hereinafter *The Sedona Principles, Third Edition*].

instances where courts have considered cost shifting (Section VIII); TAR cases from foreign jurisdictions (Section IX); and considerations for using TAR in governmental investigations (Section X).

II. HISTORY OF JUDICIAL ACCEPTANCE OF TAR

A. From Da *Silva Moore* in 2012 to *Rio Tinto* in 2015

In 2012, *Da Silva Moore v. Publicis Groupe* became the first published opinion recognizing TAR as an "acceptable way to search for relevant ESI in appropriate cases."[5] The decision paved the way for practitioners to use TAR with confidence as a defensible discovery tool, and for additional courts to reinforce that principle. As the use of TAR became more common, courts have consistently opined that the acceptability of its use is well established. Moving beyond the issue of *whether* a party may use TAR, courts have confronted issues on *how* parties are using TAR. Meanwhile, how parties use TAR have also evolved in ways that impact the issues addressed by courts confronted with TAR, with a notable example of TAR 1.0 and TAR 2.0 workflows.

The court in *Da Silva Moore* approved a party-negotiated TAR protocol, which had set forth the manner of selection and review of the seed and training document sets,[6] and addressed those aspects of the protocol about which the parties disagreed.[7] The court stated that "[w]hat the Bar should take away from this Opinion is that [TAR] is an available tool and should be seriously considered for use in large-data-volume cases where it

5. *Da Silva Moore*, 287 F.R.D. at 183.

6. *Da Silva Moore* involved TAR 1.0. which refers to the use of Simple Active Learning ("SAL") and Simple Passive Learning ("SPL") protocols, both of which are single-time training protocols. *See* below for further discussion. The seed set is "[a] manually compiled set of documents used to train an analytic index for the purposes of performing some form of technologically-assisted review." *The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition*, 21 SEDONA CONF. J. 263 (2020).

7. *See Da Silva Moore*, 287 F.R.D. at 182–83, 190–93.

may save the producing party (or both parties) significant amounts of legal fees in document review."[8] The court stated, however, "[t]hat does not mean computer-assisted review must be used in all cases, or that the exact ESI protocol approved here will be appropriate in all future cases that utilize computer-assisted review."[9]

The court suggested that "the best approach" when a party wishes to use TAR is to "follow the Sedona Cooperation Proclamation model" and "[a]dvise opposing counsel that you plan to use [TAR] and seek agreement."[10] Noting the responding party's willingness to provide the requesting party with "[a]ll documents that are reviewed as a function of the seed set . . . and . . . to the extent applicable, the issue tag(s) coded for each document," the court "highly recommend[ed] that counsel in future cases be willing to at least discuss, if not agree, to such transparency in the computer-assisted review process."[11] If, however, parties cannot agree, the court stated that they should "consider whether to [either] abandon [TAR] for that case or go to the court for advance approval," noting that court approval would be unlikely absent "results [that] are quality control verified."[12] As for court approval, the court stated that it "recognizes that [TAR] is not a magic, Staples-Easy-Button, solution appropriate for all cases."[13] While the technology should be used where appropriate, courts should consider the particular protocol that is proposed. "[I]t is not a case of machine replacing

8. *Id.* at 193.

9. *Id*.

10. *Id.* at 184 (quoting Andrew Peck, *Search, Forward*, L. TECH. NEWS, Oct. 11, 2011, at 25, 29).

11. *Id.* at 192.

12. *Id*. at 184, 192.

13. *Id.* at 189.

humans: it is the process used and the interaction of man and machine that the courts need to examine."[14] The court emphasized: "While this Court recognizes that [TAR] is not perfect, the Federal Rules of Civil Procedure do not require perfection."[15]

The court concluded that defendant's use of TAR was appropriate, considering the following factors: (1) the parties' agreement to use TAR (even though they disagreed on certain aspects of its implementation); (2) "the vast amount of ESI to be reviewed (over three million documents);" (3) "the superiority of [TAR] to the available alternatives (i.e., linear manual review or keyword searches);" (4) "the need for cost effectiveness and proportionality under Federal Rule of Civil Procedure 26(b)(2)(C);" and (5) "the transparent process proposed by [defendant]."[16]

Following *Da Silva Moore*'s recognition that TAR was an acceptable search methodology, courts began encouraging the use of TAR or commenting on its potential to reduce cost and burden.[17] Some courts in these early cases encouraged (and even ordered) the parties to consider TAR.[18] And some cases, without

---

14. *Id.*

15. *Id.* at 191.

16. *Id.* at 192.

17. *See, e.g.*, Nat'l Day Laborer Org. Network v. U.S. Immigr. & Customs Enforcement Agency, 877 F. Supp. 2d 87, 111 (S.D.N.Y. 2012) (suggesting TAR could address keyword search shortcomings); *In re* Domestic Drywall Antitrust Litig., 300 F.R.D. 228, 233 (E.D. Pa. 2014) (noting use of technology could lead to greater efficiency and more beneficial results); Malone v. Kantner Ingredients, Inc., No. 4:12CV3190, 2015 WL 1470334, at *3 n.7 (D. Neb. Mar. 31, 2015).

18. *See, e.g.*, FDIC v. Bowden, No. CV413-245, 2014 WL 2548137, at *13 (S.D. Ga. June 6, 2014) (ordering parties to consider the use of TAR); Aurora Coop. Elevator Co. v. Aventine Renewable Energy-Aurora W. LLC, No. 4:12CV230, 2015 WL 10550240, at *1 (D. Neb. Jan. 6, 2015) (ordering the parties to "consult with a computer forensic expert to create search protocols, including predictive coding as needed, for a computerized review of the

engaging in substantive discussions, noted the parties' use of TAR in reviewing productions of opposing parties or non-parties.[19] In these earliest cases, before the acceptance of TAR was well established, cooperation and agreement by parties on both sides initially weighed heavily into courts' approval of TAR.[20]

Courts soon began referring to the use of TAR as a well-accepted methodology. The court in *Dynamo Holdings Ltd. Partnership v. Commissioner of Internal Revenue* (*Dynamo Holdings I*), for example, rejected the requesting party's assertion that TAR is an "unproved technology," noting that "the understanding of e-discovery and electronic media has advanced significantly in the last few years, thus making predictive coding more acceptable in the technology industry than it may have previously been."[21] The court added that "[i]n fact, we understand that the

---

parties' electronic records"); Johnson v. Ford Motor Co., No. 3:13-cv-06529, 2015 WL 4137707, at *11 (S.D. W. Va. July 8, 2015) (ordering the parties to "involve their IT experts and to consider other methods of searching such as predictive coding").

19. N.M. State Invest. Council v. Bland, No. D-101-CV-2011-01534, 2014 WL 772860 (D.N.M. Feb. 12, 2014); Arnett v. Bank of Am., N.A., No. 3:11-cv-1372-SI, 2014 WL 4672458 (D. Or. Sept. 18, 2014).

20. *See Da Silva Moore*, 287 F.R.D. at 193 (negotiated protocol); Kleen Prods. LLC v. Packaging Corp. of Am., No. 10 C 5711, 2012 WL 4498465 (N.D. Ill. Sept. 28, 2012) (ordering parties to cooperate where a requesting party sought to require responding party to use TAR); Fed. Hous. Fin. Agency v. JPMorgan Chase & Co., No. 1:11-cv-06188-DLC (S.D.N.Y. July 24, 2012) (Transcript at 9, 14) (appearing to encourage disclosure of the training sets by stating that for the TAR process to work, "it needs transparency and cooperation of counsel"); Rio Tinto PLC v. Vale S.A., 306 F.R.D. 125, 129 (S.D.N.Y. 2015) (noting the level of transparency required for certain workflows was not established but did not need to be decided because the parties had agreed to a protocol addressing the issue).

21. Dynamo Holdings Ltd. P'ship v. Comm'r of Internal Revenue (Dynamo Holdings I), 143 T.C. 183, 191–92 (2014) (citing *Da Silva Moore*, 287 F.R.D at 182 n.2, *adopted sub nom.*, Da Silva Moore v. Publicis Groupe SA, No. 11 Civ. 1279 (ALC)(AJP), 2012 WL 1446534 (S.D.N.Y. Apr. 26, 2012)); *see also*

technology industry now considers predictive coding to be widely accepted for limiting e-discovery to relevant documents and effecting discovery of ESI without an undue burden."[22] Many courts have also commented on TAR as a means to reduce cost and burden.[23]

In *Rio Tinto PLC v. Vale S.A.*, decided in 2015, the court observed that "[i]n the three years since *Da Silva Moore*, the case law has developed to the point that it is now black letter law that where the producing party wants to utilize TAR for document review, courts will permit it."[24] The court pointed to a long

---

Progressive Cas. Ins. Co. v. Delaney, No. 2:11-cv-00678-LRH-PAL, 2014 WL 3563467, at *8 (D. Nev. July 18, 2014) (providing citations of articles indicating that TAR has proved to be an accurate way to comply with a discovery request for ESI and that studies show it is more accurate that human review or keyword searches); *FDIC v. Bowden*, 2014 WL 2548137, at *13 (S.D. Ga. June 6, 2014) (directing that the parties consider the use of TAR).

22. *Dynamo Holdings I*, 143 T.C. at 192.

23. *See*, e.g., Harris v. Subcontracting Concepts, LLC, No. 1:12-MC-82 (DNH/RFT), 2013 WL 951336, at *5 (N.D.N.Y. Mar. 11, 2013) (noting TAR, along with other recent technologies, can dramatically reduce the time and cost of production); *see also* Chevron Corp. v. Donziger, No. 11 Civ. 0691(LAK), 2013 WL 1087236, at *32 n.255 (S.D.N.Y. Mar. 15, 2013); Zhulinska v. Niyazov Law Grp., P.C., No. 21-CV-1348 (CBA), 2021 WL 5281115, at *3 (E.D.N.Y. Nov. 12, 2021); Republic of the Gambia v. Facebook, Inc., No. 20-mc-36-JEB-ZMF, 567 F. Supp. 3d 291 (D.D.C. 2021), *vacated in part sub nom.* Republic of the Gambia v. Facebook, Inc., 575 F. Supp. 3d 8 (D.D.C. 2021), *reconsideration denied sub nom*. Republic of the Gambia v. Meta Platforms, Inc., No. 20-36 (JEB), 588 F. Supp. 3d 1 (D.D.C. 2022).

24. *Rio Tinto*, 306 F.R.D. at 127, 129 (S.D.N.Y. 2015) ("One point must be stressed—it is inappropriate to hold TAR to a higher standard than keywords or manual review. Doing so discourages parties from using TAR for fear of spending more in motion practice than the savings from using TAR for review").

list of cases in which courts had approved the responding party's use of TAR during the period of 2012-15.[25]

B. Emergence of TAR 2.0

As TAR has become more widely used, TAR technologies, uses, and workflows have also evolved. A particularly notable development has been workflows using TAR 2.0, also referred to as "Continuous Active learning" ("CAL"),[26] and other terms, which have affected issues that may arise between parties and resulting case law. The terms "TAR 1.0" and "TAR 2.0," which have their genesis as marketing terms, refer to contrasting TAR workflow methodologies. The earlier of the TAR workflows to emerge, often known as TAR 1.0, refers to the use of discrete training sets within the entire review population.[27] Then, counsel may or may not engage in further responsiveness review of the categorized documents. By contrast, TAR 2.0 refers to a

---

25. *See id.* at 127–28 (citing *Dynamo Holdings I*, 143 T.C. 9); Green v. Am. Modern Home Ins. Co., No. 1:14–cv–04074, 2014 WL 6668422, at *1 (W.D. Ark. Nov. 24, 2014); Aurora Coop. Elevator Co. v. Aventine Renewable Energy– Aurora W. LLC, No. 12 Civ. 0230, ECF No. 147 (D. Neb. Mar. 10, 2014); Edwards v. Nat'l Milk Producers Fed'n, No. 11 Civ. 4766, ECF No. 154 (N.D. Cal. Apr. 16, 2013) (Joint Stip. & Order); Bridgestone Ams., Inc. v. Int'l Bus. Machs. Corp., No. 3:13–1196, 2014 WL 4923014 (M.D. Tenn. July 22, 2014); Fed Hous. Fin. Agency v. HSBC N.A. Holdings, Inc., Nos. 11 Civ. 6189(DLC), 2014 WL 584300, at *3 (S.D.N.Y. Feb. 14, 2014); EORHB, Inc. v. HOA Holdings LLC, No. 7409-VCL, 2013 WL 1960621 (Del. Ch. May 6, 2013); *In re* Actos (Pioglitazone) Prods. Liab. Ltg., 274 F. Supp. 3d 485 (W.D. La. 2017).

26. The terms "continuous active learning "and "CAL" are trademarks of Maura Grossman and Gordon Cormack. *See* Gordon V. Cormack & Maura R. Grossman, *Evaluation of Machine Learning Protocols for Technology-Assisted Review in Electronic Discovery*, in SIGIR '14: Proceedings of the 37th international ACM SIGIR conference on Research & development in information retrieval, at 153–62 (July 3, 2014), *available at* http://dx.doi.org/10.1145/2600428.2609601 ("SIGIR study").

27. *Id*.

workflow where, generally, every document the TAR model identifies as most likely to be responsive is prioritized for review by human reviewers, and their coding further trains the algorithm.[28]

The TAR 2.0 workflow was first discussed in *Rio Tinto*. There, the court discussed the evolution of TAR technologies and workflows and how those changes impacted parties' discussions about TAR, including, for example, some requesting parties' concerns about the composition of seed and training sets.[29] The *Rio Tinto* court noted studies showing that with TAR tools employing this distinct "continuous active learning" workflow, the seed set may have little or no impact, and that as a practical matter, there may be no discrete training sets to share.[30]

28. While this generally describes a TAR 2.0 review for responsiveness, variations to this workflow exist.

29. While "training" documents refer to any documents used as inputs to create a TAR model, "seed" documents is a term used less consistently. While it commonly refers to the set of training documents selected for the first run of a TAR algorithm to build a model, it is sometimes used to refer to a broader set of training documents. *See, e.g.*, Winfield v. City of New York, No. 15-CV-05236 (LTS)(KHP), 2017 WL 5664852, at *4 (S.D.N.Y. Nov. 27, 2017) ("For TAR to work properly, the producing party must prepare a training, or seed set, of responsive and non-responsive documents to train the computer system how to distinguish between them.").

30. Rio Tinto PLC v. Vale S.A., 306 F.R.D. 125, 128 (S.D.N.Y. 2015) (citing SIGIR study).

III. COURT INVOLVEMENT IN TAR

Court involvement relating to TAR most commonly occurs when courts enter TAR protocols that the parties have negotiated and stipulated.[31] Court involvement also has occurred when a responding party seeks court approval of its unilateral decision to use TAR or the methodology it intends to use. It has also occurred when a requesting party seeks to compel a responding party to use TAR or implement a specific TAR protocol. Although rare, courts have sua sponte ordered the use of TAR.

A. Permission Not Needed for Responding Party to Use TAR

Generally, as discussed further in Section III.C below, a responding party may not only determine how and whether to use TAR, it may do so without seeking court permission.[32] In *Entrata, Inc. v. Yardi Systems, Inc.*, the court denied the plaintiff's motion to compel disclosure of the complete methodology and results of the defendant's TAR process in a situation where the parties failed to reach agreement on search methodology early on and where the plaintiff knew about the use of TAR but did

31. At times, courts are also involved in crafting provisions of TAR protocols.

32. While early cases such as *Da Silva Moore v. Publicis Groupe*, 287 F.R.D. 182, 184 (S.D.N.Y. 2012) stressed the importance of party agreement or court approval, this requirement no longer applied after "the case law has developed to the point that it is now black letter law that where the producing party wants to utilize TAR for document review, courts will permit it." *Rio Tinto*, 306 F.R.D. at 127. As discussed in Section VI, the exception to this general practice is where parties deviate from the negotiated ESI protocol in implementing TAR.

not take issue with it until the last day of discovery.[33] The court noted that it was "'black letter law' that courts will permit a producing party to utilize TAR" and that the plaintiff "was not required to seek approval from the Magistrate Court to use TAR where there was never an agreement to utilize a different search methodology."[34] Citing *Entrata*, *In re Broiler Chicken Grower Antitrust Litigation (No. II)*, similarly held, "Courts in this district have found that when there has not been an agreement to the contrary, a party is not required to seek approval to use TAR."[35]

The court in *Dynamo Holdings I* likewise opined that responding parties need not seek court permission to use TAR, and that the requesting party can object after production if the production is not complete. It explained that responding parties are generally free to decide their own process for discovery without needing prior judicial approval.[36]

In *William Morris Endeavor Entertainment, LLC v. Writers Guild of America West, Inc.*, the court similarly found that court approval of the use of TAR was not necessary.[37] The court,

---

33. Entrata, Inc. v. Yardi Sys., Inc., No. 2:15-cv-00102, 2018 WL 5470454, at*7 (D. Utah Oct. 29, 2018).

34. *Id.*, quoting *Rio Tinto* at 127. Further discussion of *Entrata* is in Section IV.A.

35. *In re* Broiler Chicken Grower Antitrust Litig. (No. II) (*In re* Boiler Chicken II), No. 6:20-2977-RJS-CMR, 2022 WL 2812679, at *2 (E.D. Okla. Feb. 7, 2022).

36. Dynamo Holdings I, 143 T.C. 183, 188–89 (2014) ("[T]he Court is not normally in the business of dictating to parties the process that they should use when responding to discovery. If our focus were on paper discovery, we would not (for example) be dictating to a party the manner in which it should review documents for responsiveness or privilege, such as whether that review should be done by a paralegal, a junior attorney, or a senior attorney.").

37. William Morris Endeavor Ent., LLC v. Writers Guild of Am. W., Inc, No. 219CV05465ABAFMX, 2020 WL 6162797, at *2 (C.D. Cal. June 8, 2020)

however, did note that the defendants should be prepared to defend [their search] plan if later challenged by [plaintiffs]."[38]

Finally, in *Bliss v. CoreCivic, Inc.*, the court commented in dicta when ruling on a proposed scheduling order that it "need not be involved" in the defendant's "ordinary" decision to use TAR, unless there existed some "basis to believe that the mechanism used is either purposefully or inherently failing to identify proportional, relevant, and responsive ESI."[39]

B. Whether Court May Compel TAR

While courts generally find that TAR is an acceptable methodology for responding parties to use, courts generally decline to *require* responding parties to use TAR to fulfill their discovery obligations.

1. Courts Declining to Order TAR

Kleen Products LLC v. Packaging Corporation of America was one of the first cases in which a court considered the issue of imposing the use of TAR on a responding party.[40] In *Kleen*, the plaintiffs sought to require defendants to use TAR rather than (according to the plaintiffs) the "antiquated Boolean [] search of [defendants'] self-selected custodians' ESI and certain central files."[41] The defendants objected because they had already used

---

38. *Id.*

39. Bliss v. CoreCivic, Inc., No. 2:18-cv-01280-JAD-EJY, 2021 WL 930692, at *1 (D. Nev. Feb. 9, 2021). *But see In re* Diisocyanates Antitrust Litig., No. 18-1001, MDL No. 2862, 2021 WL 4295729 (W.D. Pa. Aug. 23, 2021) *adopted by In re Diisocyanates*, 2021 WL 4295719 (W.D. Pa. Sept. 21, 2021) (finding process to be unreasonable and sent parties back to the drawing board).

40. Kleen Prods. LLC v. Packaging Corp. of Am., No. 10-cv-5711, 2012 WL 4498465 (N.D. Ill. Sept. 28, 2012).

41. *Kleen Prods.*, Plaintiffs' Statement of Position with Respect to Disputed Items for Dec. 15, 2011 Status Conference at 4–5, ECF No. 266 (N.D. Ill. Dec. 13, 2011).

keyword searches and viewed TAR as a "new, untested document gathering and production protocol."[42] After holding evidentiary hearings on the efficacy of TAR,[43] the court ultimately declined to require the defendants to adopt one methodology over another. Instead, the court ordered the parties to meet and confer regarding modifications to the responding party's existing search methodology.[44]

In *Hyles v. New York City*, the court held that defendant New York City could not be compelled to use TAR against its will even though the court agreed that, "in general, TAR is cheaper, more efficient and superior to keyword searching."[45] Unlike prior cases, where the responding party had already expended significant effort and expense on document review and production,[46] in *Hyles* the responding party had not yet commenced its review. This raised the issue of whether, on the requesting party's motion to compel the use of TAR at the outset of discovery, the court would order the responding party to use TAR. It

---

42. *See Kleen Prods.*, Defendants' Statement of Position with Respect to Disputed Items for Dec. 15, 2011 Status Conference at 3, ECF No. 267 (N.D. Ill. Dec. 13, 2011).

43. *See Kleen Prods.*, (N.D. Ill. Mar. 1, 2012) (Feb. 21, 2012 Transcript); *Kleen Prods.*, (N.D. Ill. Aug. 2, 2012) (Mar. 28, 2012 Transcript).

44. *Kleen Prods.*, (Aug. 2, 2012) (Mar. 28, 2012 Transcript). Ultimately, the parties stipulated that plaintiffs could object to defendants' search methodology and propose alternatives but would withdraw their request for TAR. Stipulation & Order Relating to ESI Search, *Kleen Prods.*, (Aug. 21, 2012); *see also Kleen Prods.*, 2012 WL 4498465 (N.D. Ill. Sept. 28, 2012).

45. Hyles v. New York City, No. 10 Civ . 3119 (AT)(AJP), 2016 WL 4077114, at *2 (S.D.N.Y. Aug. 1, 2016).

46. The court stated that in prior cases "where the requesting party has sought to force the producing party to use TAR, the courts have refused." *Id*. The court noted, however, that in those cases, the responding party had already "spent over $1 million using keyword search (in *Kleen [Products]*) or keyword culling followed by TAR (in *Biomet*)." *Id.* (emphasis added).

declined to do so. The court held that "it is not up to the Court, or the requesting party (Hyles), to force the City as the responding party to use TAR when it prefers to use keyword searching."[47] The court explained that while the requesting party "may well be correct that production using keywords may not be as complete as it would be if TAR were used," nevertheless "the standard is not perfection, or using the 'best' tool," but rather "whether the search results are reasonable or proportional."[48] The court concluded that there "may come a time when TAR is so widely used that it might be unreasonable for a party to decline to use TAR," but "[w]e are not there yet."[49]

Similarly, in *In re Viagra (Sildenafil Citrate) Products Liability Litigation*, the court denied the plaintiffs' request that defendant use TAR and that the plaintiffs' representatives be involved in the defendant's TAR process.[50] The defendant instead planned to use an iterative search-term process, which it would test and validate through sampling. Relying on *Hyles*, the court in *Viagra* held that it was not up to the court or the requesting party to force a responding party to use TAR when it preferred to use search terms. The court reasoned that it would not compel the use of TAR, even if it were a superior method, absent evidence of insufficient discovery responses.[51] The court therefore denied the motion without prejudice.

---

47. *Id*. at *3.

48. *Id*.

49. *Id*.

50. *In re* Viagra (Sildenafil Citrate) Prods. Liab. Litig., No. 16-md-02691-RS (SK), 2016 WL 7336411 (N.D. Cal. Oct. 14, 2016).

51. *Id.* at *2.

In re Mercedes-Benz Emissions Litigation echoed that reasoning when it declined to compel the use of TAR.[52] In that case, the plaintiffs moved to compel the defendants to use TAR to identify responsive documents, arguing that TAR "yields significantly better results than either traditional human 'eyes on' review of the full data set or the use of search terms."[53] The defendants objected, preferring instead to use custodians and search terms to identify relevant documents and arguing that there was no authority for a court to require TAR.[54] In addition, the defendants claimed that using TAR would not be appropriate in light of certain ESI issues present in the case, including language and translation, unique acronyms and identifiers, redacted documents, and technical documents that would make TAR challenging and ineffective.[55]

The special master noted that while the benefits of TAR are widely recognized, no court had compelled a party to use TAR over objection.[56] Despite his view that TAR would be the "more cost effective and efficient methodology," the special master allowed the defendant to use its preferred custodian-and-search-term approach.[57]

---

52. *In re* Mercedes-Benz Emissions Litig., No. 2:16-cv-881 (KM) (ESK), 2020 WL 103975 (D.N.J. Jan. 9, 2020). For further discussion about this case, see Section III.C. *See also* Raymond James & Assocs., Inc. v. 50 N. Front St. TN, LLC, No. 18-cv-2104-JTF-tmp, 2022 WL 3337275, at *4 (W.D. Tenn. Feb. 8, 2022) (citing *In re Mercedes-Benz* and refusing to find that costs incurred from manual review were unreasonable where plaintiff did not use TAR).

53. *In re Mercedes-Benz*, 2020 WL 103975, at *1.

54. *Id*.

55. *Id*.

56. *Id*.

57. *Id*. at *2; *see also In re* Bridgepoint Educ., Inc. Sec. Litig., No. 12cv1737 JM (JLB), 2014 WL 3867495 (S.D. Cal. Aug. 6, 2014) (denying plaintiffs' request to require defendants to use TAR on documents that defendants had previously searched using traditional search terms); Klein v. Facebook, Inc.,

2. Courts Ordering TAR

Three decisions have ordered the use of TAR, in the context of ongoing discovery problems caused, at least in part, by the responding party's conduct. In *Independent Living Center v. City of Los Angeles*, the court ordered the use of TAR to search more than two million documents after "little or no discovery was completed" before the discovery cutoff, and the parties had ongoing disputes after "months of haggling" over search terms that yielded large numbers of documents for review.[58]

In *OSI Restaurant Partners v. United Ohana*, the Delaware Court of Chancery granted the defendant's motion to compel in part, ordering the plaintiff to identify responsive documents by applying TAR to all produced documents that had not previously undergone a document-by-document attorney-level review for responsiveness.[59] The court further directed that the parties work together, with their eDiscovery vendors, to develop a TAR process; that the plaintiff implement the TAR process; and that the plaintiff make a new production to the defendants.[60] In addition, the court stated that the plaintiff would be responsible for all expenses associated with the TAR process.[61]

Similarly, in *Winfield v. City of New York*, after "numerous complaints about the pace of discovery and document review, which initially involved only manual linear review of documents," the court ordered the responding party to begin using

---

No. 20-cv-08570-LHK (VKD), 2021 U.S. Dist. LEXIS 175738, at *8 (N.D. Cal. Sep. 15, 2021) (noting that the court may not require a party to adopt a particular TAR protocol).

58. Indep. Living Center v. City of Los Angeles, No. 2:12-cv-00551, Minute Order at 1, ECF 375 (C.D. Cal. June 26, 2014).

59. OSI Rest. Partners, LLC v. United Ohana, LLC, No. 12353-CB, 2017 WL 396357 (Del. Ch. Jan. 27, 2017).

60. *Id.* at *2.

61. *Id*.

TAR "to hasten the identification, review, and production of documents responsive to Plaintiffs' document requests."[62]

3. Courts Suggesting TAR

Courts sometimes suggest to the parties that the use of TAR may be appropriate to address discovery issues. For instance, in *EORHB, Inc. v. HOA Holdings LLC*, the Delaware Court of Chancery sua sponte ordered the parties to use TAR or, alternatively, to show cause why TAR should not be used.[63] The defendant ultimately elected to use TAR. The plaintiff, however, was not required to do so after informing the court that because of the low volume of documents it expected to have to review and produce, the cost of using TAR likely would outweigh any practical benefits.[64]

Similarly, in granting the plaintiff's motion to compel in a short one-page order, the court in *Davine v. Golub Corporation* expressly stated that the defendants could continue to rely on their TAR model in conducting its review of the compelled documents from newly identified custodians.[65] It likewise ordered that the defendants could "cease their review of the documents identified as possibly relevant when they made a good faith determination that the burden of continuing the review outweighs the benefit in terms of identifying relevant documents."[66]

---

62. Winfield v. City of New York, 15-CV-05236 (LTS) (KHP), 2017 WL 5664852, at *4 (S.D.N.Y. Nov. 27, 2017).

63. EORHB, Inc. v. HOA Holdings LLC, No. 7409-VCL (Del. Ch. Oct. 15, 2012) (Hearing Transcript at 66–67).

64. *See EORHB, Inc. v. HOA Holdings LLC*, No. 7409-VCL, 2013 WL 1960621 (Del. Ch. May 6, 2013).

65. Davine v. Golub Corp., No. 3:14-cv-30136-MGM, 2017 WL 549151, at *1 (D. Mass. Feb. 8, 2017).

66. *Id*.

The court likewise suggested the use of TAR to address overbroad discovery in *Story v. Fiat Chrysler Automotive*, a race discrimination and retaliation case brought by an employee against his employer.[67] There, the plaintiff moved to compel discovery, claiming that the defendant's responses to his interrogatories and requests for production of documents were incomplete.[68] The defendant objected to the document request that called for all documents and emails pertaining to or about the plaintiff for an 18-month time period, arguing that the request was too expansive and not proportional to the needs of the case.[69] The court agreed but encouraged counsel to consider "key word searches or technology assisted review . . . to narrow the volume of an otherwise overly-broad request."[70]

The court in *Youngevity International Corporation v. Smith* encouraged the use of TAR from an early stage of discovery, suggesting that TAR might be an appropriate option in the case and instructing defense counsel to determine the cost of TAR to sort responsive from nonresponsive documents.[71]

---

67. Story v. Fiat Chrysler Auto., No. 4:17-CV-12, 2018 WL 5307230 (N.D. Ind. Oct. 26, 2018).

68. *Id.* at *1.

69. *Id.* at *2.

70. *Id.* at *3.

71. Youngevity Int'l Corp. v. Smith, No. 16-cv-00704-BTM (JLB), 2019 WL 1542300, at *8, 15 (S.D. Cal. Apr. 9, 2019) (instructing counsel to find out the cost of TAR and then ordering the parties confer about it), report *adopted sub nom.* Youngevity Intl. v. Smith, No. 16-cv-704-BTM-JLB, 2019 WL 11274846 (S.D. Cal. May 28, 2019).

C. Challenges to Responding Party's TAR Methodology

1. Discretion to Responding Party and Sedona Principle 6

In addition to having discretion over whether to use TAR, responding parties typically may select the methodology they use for their TAR process without judicial involvement, provided that it is reasonable. When addressing TAR issues, courts have frequently relied on and cited Principle 6 of The Sedona Principles, which states:

> Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.[72]

These cases reflect that, as with other discovery issues, courts will apply Sedona Principle 6 to defer to a responding party's chosen methodologies when they are reasonable. Courts applying Principle 6 have declined to intervene in a responding party's decisions on whether and how to use TAR, unless a requesting party can show a specific deficiency in a responding party's production or unreasonableness of the selected process.

For example, Sedona Principle 6 was key to the holding in *Livingston v. City of Chicago*, where the court allowed the defendant to use TAR and declined to order the defendant to consult the plaintiff when establishing a review protocol.[73] The parties disagreed about whether it was appropriate to apply keyword

72. *The Sedona Principles, Third Edition*, *supra* note 3, Principle 6.

73. Livingston v. City of Chicago, No. 16 CV 10156, 2020 WL 5253848 (N.D. Ill. Sept. 3, 2020). Further discussion of this case can be found in Sections IV.B, V.A, and VI.A.

culling to the dataset prior to applying TAR.[74] The court found that the City's TAR proposal was reasonable under the federal rules and, citing Sedona Principle 6, held that the City is "best situated to decide how to search for and produce [responsive] emails . . . ."[75] The court also declined to direct the responding party's TAR process, where its proposed methodology "satisfies the reasonable inquiry standard and is proportional to the needs of this case under the federal rules."[76]

In *Coventry Capital US LLC v. EEA Life Settlements Inc.*, the parties generally agreed to use TAR but disagreed about the specific protocols to be used, leading to a "protracted and contentious" TAR review process.[77] Noting the responding party's representations that its manual review of the disputed ESI subset could be completed within three weeks and that the addition of that data would "skew the recall and precision metrics and cause delay," the court allowed the responding party to exclude that population from TAR review.[78] Declining to "force" TAR on the responding party at such a "late stage of Phase I of discovery," the court rejected the requesting party's argument that manual review of the ESI in dispute would cause further delay.

Similarly in *Lawson v. Spirit AeroSystems, Inc.*, the court rejected the plaintiff's complaints about the specific recall the

74. *Id*.

75. *Id.* at *3.

76. *Id*.

77. Coventry Cap. US LLC v. EEA Life Settlements Inc., No. 17-Civ. 7417 (VM) (SLC), 2020 WL 7383940, at *4 (S.D.N.Y. Dec. 16, 2020), *objections overruled*, 2021 WL 961750 (S.D.N.Y. Mar. 15, 2021).

78. *Id.* at *6 (noting that, although courts generally permit a responding party to use TAR, "where the requesting party has sought to force the producing party to use TAR, the courts have refused") (internal quotations omitted) (citing Rio Tinto PLC v. Vale S.A., 306 F.R.D. 125, 127 n.1 (S.D.N.Y. 2015)). Recall and precision are defined and discussed in Section V.C.

defendant used in its TAR process, explaining that the defendant's TAR review process was reasonable, and that the plaintiff's motion to compel the additional review of residual documents was disproportionate to the needs of the case.[79]

Relying on Principle 6, the court in *Kaye v. New York City Health and Hospitals Corp.* held there was no basis to compel an inquiry into the search methodology of a responding party that used TAR where the requesting party had not identified any deficiency in the production.[80] The court ruled that a requesting party is not entitled, in the first instance, to conduct discovery about the responding party's production methodology, and that any such inquiry must be based on identification of some deficiency and must be proportional to the facts and circumstances of the case.[81]

As discussed in the next section, Principle 6 does not provide responding parties with unlimited discretion to make unreasonable discovery choices.[82] Further, stipulated ESI protocols

---

79. Lawson v. Spirit AeroSystems, Inc., No. 18-1100-EFM-ADM, 2020 WL 1813395, at *8–9 (D. Kan. Apr. 9, 2020). As in prior cases, the court recognized that TAR is widely accepted under the law. *Id.* at *6 (citing, among other authorities, Da Silva Moore v. Publicis Groupe, 287 F.R.D. 182, 183 (S.D.N.Y. 2012) and *The Sedona Conference Glossary E-Discovery and Digital Information Management*, *Fourth Edition*, 15 SEDONA CONF. J. 305 (2014)). Further discussion of *Lawson* can be found in Sections V.C. and VIII.B.

80. Kaye v. N.Y.C. Health and Hospitals Corp., No. 18-CV-12137 (JPO) (JLC), 2020 WL 283702 (S.D.N.Y. Jan. 21, 2020).

81. *Id.* at *3–4.

82. *In re* Diisocyanates Antitrust Litig., No. 18-1001, 2021 WL 4295729, at *8–12 (W.D. Pa. Aug. 23, 2021) (special master finding that while Principle 6 does allow the responding party to decide in the first instance how it will produce its documents, it did not entitle the responding party to proceed with a proposed TAR methodology that contained "serious flaws" and was "not reasonable"), *adopted by In re Diisocyanates*, 2021 WL 4295719, at *2 (W.D. Pa. Sept. 21, 2021).

between the parties, when ordered by the court, can take priority over general principles of deference to the responding party's decision on appropriate use of TAR.[83]

2. No Discretion to Responding Party for Unreasonable Process

While courts generally do not direct how a responding party uses TAR, "[t]his general rule does not, however, give carte blanche to a producing party" and courts may require parties to redesign unreasonable processes.[84] The parties in *In re Diisocyanates Antitrust Litigation* generally agreed to the use of TAR, but they disagreed over the specific TAR protocols to be used.[85] The court adopted the special master's report and recommendation, which rejected the defendant's motion to permit it to follow a TAR protocol that was determined to be unreasonable because its validation process was flawed.[86] The court stated that the special master provided "a roadmap highlighting the potholes in Defendants' prior positions and how to proceed to achieve reasonable and proportionate search terms and TAR methodologies."[87] The defendants were free to conduct their review consistent with the special master's guidance and were "not compelled to adopt Plaintiffs' search terms or TAR methodologies."[88] Later, after Defendants asserted they had

83. *In re* Valsartan, Losartan, & Irbesartan Prods. Liab. Litig., 337 F.R.D. 610, 617 (D.N.J. 2020) (holding the defendant had violated the court-ordered ESI protocol by "not timely disclosing its use or possible use" of TAR, and therefore requiring defendant to follow plaintiff's proposed TAR methodology instead of defendant's own).

84. *In re Diisocyanates*, 2021 WL 4295729, at *6.

85. *Id.* at *9–10.

86. *In re Diisocyanates*, 2021 WL 4295719, at *1 (W.D. Pa. Sept. 21, 2021).

87. *Id*.

88. *Id*.

completed their TAR review, the special master required some defendants to conduct additional review, based on a qualitative and quantitative evaluation that showed their decision to stop was not reasonable.[89]

Additionally, some courts have cautioned that parties also bear any risks if their process is less efficient than TAR or results in deficiencies. For example, in *In re Mercedes-Benz*, the special master denied the plaintiffs' motion to compel the defendants to use TAR, holding that "Defendants may evaluate and decide for themselves the appropriate technology for producing their ESI."[90] The special master cautioned, however, that he would "not look favorably on any future arguments related to burden of discovery requests, specifically cost and proportionality, when Defendants have chosen to utilize the custodian-and-search term approach despite wide acceptance that TAR is cheaper, more efficient and superior to keyword searching."[91] In addition, the court noted that once the production was made, the plaintiffs could renew their request to compel the use of TAR if the defendants' production was, in fact, deficient.[92]

Similarly, the court required certain disclosures of the responding party relating to the appropriateness of the search

89. *In re Diisocyanates*, 2022 WL 17668470, *24–29 (W.D. Pa. Oct. 19, 2022), *modified by In re Diisocyanates*, ECF No. 800 (W.D. Pa. Oct. 21, 2022).

90. *In re* Mercedes-Benz Emissions Litig., No. 2:16-cv-881 (KM) (ESK), 2020 WL 103975, at *2 (D.N.J. Jan. 9, 2020); *see also id.* at *1 (citing Hyles v. New York City, No. 10-CIV-3119, 2016 WL 4077114, at *3 (S.D.N.Y. Aug. 1, 2016) (citing *The Sedona Principles, Second Edition: Best Practices & Principles for Addressing Electronic Document Production*, Principle 6)). Further discussion of this case can be found in Sections III.B.

91. *In re Mercedes-Benz*, 2020 WL 103975, at *2.

92. *Id.* at *2–3.

process in *Winfield v. City of New York*.[93] There, the plaintiffs objected to various aspects of the defendant's document review process, which included the use of TAR for certain custodians.[94] The court disagreed with the plaintiffs' contention that the defendants' TAR process was defective.[95] Rather, the court concluded, based on its own in camera review of the City's submission, that the City "appropriately trained and utilized its TAR system."[96] The court found that five of 20 documents submitted by the City were incorrectly coded during the initial review but determined that human error in coding a small subset of documents was not enough to draw into question the accuracy of the City's TAR system, particularly since the training set comprised over 7,000 documents.[97] Moreover, the City provided information about the training of reviewers and the search criteria used and submitted to in camera review, which was enough to overcome the plaintiffs' challenge to its TAR system.[98] Like many other courts, *Winfield* explained that reasonableness, rather than perfection, is the standard in discovery.[99]

---

93. Winfield v. City of New York, No. 15-CV-05236 (LTS) (KHP), 2017 WL 5664852 (S.D.N.Y. Nov. 27, 2017).

94. *Id.* at *2.

95. While it rejected plaintiffs' claim that the city's TAR system was defective overall, the court granted the plaintiffs' motion in part, ordering the city to provide the plaintiffs with a random sample of nonresponsive documents from the review populations to increase transparency. *Id.* at *11.

96. *Id*. at *10.

97. *Id*. at *11. *See also* Section II.B.

98. *Id*.

99. *Id*. at *9.

IV. TRANSPARENCY AND DISCLOSURE

For responding parties using TAR, courts generally encourage, but do not necessarily require, cooperation, transparency, or disclosure of the fact that TAR is being used, metrics and processes involved in the TAR review, or sharing of which documents were used in training or validation. Cases that have required disclosures generally involve a demonstrated production deficiency; misconduct that requires disclosures to further assess the responding party's process; or disregard of an ESI protocol that does not permit TAR.

A. Courts Encourage Cooperation and Transparency for TAR

Courts have generally encouraged parties to disclose their intended use of TAR. While early cases tended to emphasize that parties' cooperation in TAR cases weighed in favor of the court accepting use of TAR,[100] later cases have continued to encourage cooperation and transparency while also holding that a responding party generally does not have any duty in this regard. The emergence of TAR 2.0 complicated disclosure because seed and training sets became less meaningful than in TAR 1.0.[101]

---

100. *See*, *e.g.*, Progressive Cas. Ins. Co. v. Delaney, No. 2:11-cv-00678-LRH-PAS, 2014 WL 3563467, at *10 (D. Nev. Jul. 18, 2014) ("[T]echnology assisted review of ESI [does] require[] an unprecedented degree of transparency and cooperation among counsel in the review and production of ESI responsive to discovery requests.").

101. *See* Section II.B. With the evolution of TAR technology from only TAR 1.0 to also include TAR 2.0, "the contents of the seed set [have become] much less significant." Rio Tinto PLC v. Vale S.A., 306 F.R.D. 125, 128; *see also* Maura R. Grossman & Gordon V. Cormack, *Comments on "The Implications of Rule 26(g) on the Use of Technology-Assisted Review*," 7 FED. CTS. L. REV. 285, 298 (2014).

The court in *Da Silva Moore* stated that "the best approach" if a party wants to use TAR "is to follow the Sedona Cooperation Proclamation model," "[a]dvise opposing counsel that you plan to use [TAR] and seek agreement . . . ."[102] The defendant voluntarily agreed to provide the plaintiffs' counsel with all nonprivileged relevant and nonrelevant seed-set documents. The court recommended "that counsel in future cases be willing to at least discuss, if not agree to, such transparency in the [TAR] process."[103] This "transparency allows . . . opposing counsel (and the Court) to be more comfortable with [TAR], reducing fears about the so-called 'black box' of the technology."[104] *Da Silva Moore*,[105] *Bridgestone Americas, Inc. v. International Business Machines Corp.*,[106] and *Federal Housing Finance Agency v. JP Morgan Chase & Co.*[107] all involved responding parties voluntarily agreeing to disclose either a sample (or more) from the training or validation sets. Further, in both *Da Silva Moore* and *Dynamo*

---

102. Da Silva Moore v. Publicis Groupe, 287 F.R.D. 182, 184 (S.D.N.Y. 2012) (quoting Andrew Peck, *Search, Forward*, L. TECH. NEWS, Oct. 2011, at 25). *But see Rio Tinto*, 306 F.R.D. 125 (noting that where parties do not agree to transparency, courts were split); Entrata, Inc. v. Yardi Sys., Inc., No. 2:15-cv-00102, 2018 WL 5470454 (D. Utah Oct. 29, 2018) (rejecting the notion that the Federal Rules of Civil Procedure and case law require transparent disclosures as a requirement to use TAR).

103. *Da Silva Moore*, 287 F.R.D. at 192.

104. *Id*.

105. *Id*.

106. Bridgestone Ams., Inc. v. Int'l Bus. Machs. Corp., No. 3:13-1196, 2014 WL 4923014 (M.D. Tenn. July 22, 2014).

107. Fed. Hous. Fin. Agency v. JPMorgan Chase & Co., Inc., No. 1:11-cv-06188-DLC (S.D.N.Y. Aug. 6, 2012) (July 24, 2012 Transcript at 14–15, 24); *see also id.* at 8–9 (commenting that the reliability of TAR depends on the process employed, particularly with respect to training the model using seed sets); Fed. Hous. Fin. Agency v. HSBC N. Am. Holdings Inc., 2014 WL 584300, at *3 (same case).

Holdings II, the responding party agreed to allow the opposing party to have some role in coding the documents used to train the TAR algorithm.[108]

While in *Rio Tinto* the court expressed its preference generally for cooperation in the disclosure of seed and training sets, it also recognized that where the parties do not agree on transparency, there are other ways to evaluate whether the training in the TAR process was done appropriately.[109] This may include, among other things, "statistical estimation of recall at the conclusion of the review as well as [determining] whether there are gaps in the production, and quality control review of samples from the documents categorized as non-responsive," i.e., null-set samples.[110]

Similarly, in *Bridgestone*, the court advised that because it was allowing a change to the discovery approach midstream to include the use of TAR after search-term culling, it "expects full openness in this matter."[111] In *Federal Housing Finance Agency*, the court appeared to encourage disclosure of the training sets by (1) stating that for the TAR process to work, "it needs transparency and cooperation of counsel;" and (2) confirming that the responding party would be voluntarily providing access to the nonprivileged documents in the seed set.[112] In *In re Biomet*

108. Dynamo Holdings Ltd. P'ship v. Comm'r. of Internal Revenue (Dynamo Holdings II), No. 2685-11, 8393-12, 2016 WL 4204067, at *3 (T.C. July 13, 2016); *Da Silva Moore*, 287 F.R.D. at 192 (the collaborative seed set training process included disclosure and agreement on issue-tagging).

109. Rio Tinto PLC v. Vale S.A., 306 F.R.D. 125 (S.D.N.Y. 2015).

110. *Id.* at 129. Recall is discussed in Section V.C.

111. *Bridgestone*, 2014 WL 4923014, at *1.

112. *Fed. Hous. Fin. Agency* (July 24, 2012 Transcript at 9, 14). *See also* Section II.B.

M2a Magnum Hip Products Liability Litigation[113] and in *Aurora Co-operative Elevator Co. v. Aventine Renewable Energy-Aurora West, LLC*,[114] while the courts expressly held that they could not require seed-set disclosure pursuant to the Federal Rules of Civil Procedure, they nevertheless encouraged the responding parties to "reconsider their position"[115] in the "cooperative spirit" encouraged by The Sedona Conference Cooperation Proclamation.[116] In addition, working cooperatively would "allay the risk of having to repeat the process" if it is later challenged and the court agrees that the "training was faulty or unreliable."[117]

Responding parties who disclose and attempt to negotiate protocols with requesting parties can be rewarded for their cooperation when a dispute arises. *Livingston* mainly concerned whether a party could compel another to *use* a certain TAR protocol, rather than *disclose* TAR methodology. On this point, the defendant's transparency as to its TAR methodology contributed in part to the court's decision to allow the defendant to proceed with its own TAR protocol over the plaintiffs' objections.[118] The defendant disclosed its intention to use a TAR protocol to narrow the review population, the identity of the TAR

---

113. *In re* Biomet M2a Magnum Hip Implant Prods. Liab. Litig. (MDL 2391), No. 3:12-MD-2391, 2013 WL 6405156, at *1 (N.D. Ind. Aug. 21, 2013).

114. Aurora Coop. Elevator Co. v. Aventine Renewable Energy-Aurora W., LLC, No. 4:12CV230, 2015 WL 10550240, at *1 (D. Neb. Jan. 6, 2015).

115. *Id.* at *2.

116. *In re Biomet*, 2013 WL 6405156, at *2.

117. *Aurora Coop. Elevator*, 2015 WL 10550240, at *2. *See also* William Morris Endeavor Ent., LLC v. Writers Guild of Am. W., Inc, No. 219CV05465ABAFMX, 2020 WL 6162797, at *2 (C.D. Cal. June 8, 2020) ("Obtaining prior agreement [of the use of TAR] may be beneficial because of the certainty it provides. . .").

118. Livingston v. City of Chicago, No. 16 CV 10156, 2020 WL 5253848, at *3 (N.D. Ill. Sept. 3, 2020). *See also* case discussion in Section III.C and Sections. V.A and VI.A.

software it intended to use, and how it intended to validate the results.[119] The court found those disclosures sufficient "to make the production transparent."[120]

B. No General Requirement to Disclose TAR Use or Process

While courts generally encourage transparency on TAR metrics and methodologies, they do not necessarily require disclosure of the TAR process[121] or nonresponsive document sets associated with training or validation. In addition, courts may consider information about a party's TAR process to be protected attorney work product. In *Winfield*, for example, the court required the defendant to submit a letter for in camera review describing its TAR process and training for document reviewers.[122] The court ultimately reasoned that such information was protected attorney work product and therefore not subject to disclosure.[123]

In *Entrata*, the court denied the requesting party's request for disclosures of the responding party's TAR process and metrics. *Entrata I* involved a defendant's motion to compel production of the complete methodology and results of the plaintiff's TAR process, claiming that it "need[ed] [plaintiff's] TAR information in order to assess the adequacy of [plaintiff's] document production, as well as [plaintiff's] document collection and review

119. *Id*.

120. *Id*.

121. *But see* Klein v. Facebook, Inc., No. 20-cv-08570-LHK (VKD), 2021 U.S. Dist. LEXIS 175738, at *8 (N.D. Cal. Sep. 15, 2021) (requiring party to disclose intent to use TAR and how it will be used or not used in conjunction with search terms).

122. Winfield v. City of New York, No. 15-CV-05236 (LTS) (KHP), 2017 WL 5664852, at *5 (S.D.N.Y. Nov. 27, 2017).

123. *Id.* at *12.

efforts."[124] The magistrate judge denied the motion, reasoning that the defendant did not provide "any specific examples of deficiencies" in the production "or any specific reason why it questions the adequacy of [plaintiff's] document collection and review."[125] The defendant also waited until the last day of fact discovery to file its motion, and "should have sought court intervention long ago" on any "specific concerns about [plaintiff's] TAR process."[126]

On review by the district judge (*Entrata II*), the court affirmed the magistrate judge's ruling, rejecting the defendant's argument that the Federal Rules of Civil Procedure and case law required the plaintiff "in the first instance, to provide transparent disclosures as a requirement attendant to its use of TAR."[127] The court distinguished the cases that the defendant cited, noting that they all involved TAR processes upon which the parties had agreed.[128] The parties' ESI Order required them to raise any questions regarding search methodology within 30 days of the Order, which had long since passed.[129] The court further reasoned that "'[t]he scope of the obligation to search for, and produce, ESI is circumscribed by Federal Rule of Civil Procedure 26(g) . . . .' [b]ut '[n]othing in Rule 26(g) obligates counsel to disclose the manner in which documents are collected, reviewed and produced in response to a discovery request.'"[130]

---

124. Entrata, Inc. v. Yardi Sys., Inc., No. 2:15-cv-00102-CW-PMW, 2018 WL 3055755, at *3 (D. Utah June 20, 2018).

125. *Id*.

126. *Id*.

127. *Entrata*, 2018 WL 5470454, at *4 (D. Utah Oct. 29, 2018).

128. *Id*. at *6–7.

129. *Id*. at *6.

130. *Id*. (quoting Karl Schieneman & Thomas C. Gricks III, *The Implications of Rule 26(g) on the Use of Technology-Assisted Review*, 7 FED. CTS. L. REV. 239, 243 (2013)). *Cf. In re* Broiler Chicken II, 2022 WL 2812679, at *1 (E.D. Okla.

Unless deficiencies are shown, courts typically resist requests for "discovery on discovery," including discovery of a responding party's TAR process. In *Kaye v. New York City Health and Hospitals*, although the defendants disclosed that they planned to use TAR 2.0 technology, the software they intended to use, the review workflow, and the validation methodology, the plaintiff requested the defendants' pre-TAR search terms and a review of the "culling" process.[131] The court declined the plaintiff's request for "discovery on discovery," citing the plaintiff's failure to meet and confer with the defendants or provide any examples of production deficiencies.[132]

The court reasoned that "whether [documents are] produced electronically or otherwise, the Court does not believe that, in the first instance, the receiving party has a right to examine and evaluate the way the production was made or require collaboration in the review protocol and validation process."[133] The court ruled that any inquiry into a responding party's methodology must be based on identification of some deficiency and

---

Feb. 7, 2022) (discussed *infra*); *see also,* Quirurgil, S.A.S. v. Hologic, Inc., No. 20-cv-10909-IT, 2022 WL 2719528 at *3 (D. Mass. Jan. 7, 2022). Based on the responding party's representation in discovery responses that it was producing "all" responsive documents, and finding no evidence the contrary, the court refused to compel any further production based only on the fact the responding party had used TAR. However, it warned, "If, however, that representation is not accurate, and Hologic has only produced responsive documents it identified through Technology Assisted Review, it should promptly amend its responses and set forth any limitations based on the review it conducted."

131. Kaye v. N.Y.C. Health & Hospitals Corp., No. 18-CV-12137 (JPO) (JLC), 2020 WL 283702, at *2 (S.D.N.Y. Jan. 21, 2020).

132. *Id*. at *1.

133. *Id*. at *2.

must be proportional to the facts and circumstances of the case.[134]

In similarly denying a request for "discovery about discovery," the court in *Edwards v. Scripps Media, Inc.* considered a motion for a protective order to prevent the plaintiff from taking a post-production 30(b)(6) deposition on nineteen topics, each with up to ten subparts.[135] The court rejected the plaintiff's request to inquire into the defendant's TAR processes, review workflows, and discovery metrics such as the total volume of ESI "collected, reviewed, and produced."[136] The court referred to precedent demonstrating that "[c]ourts have ordered 'discovery about discovery' when the record suggests that there is reason to distrust the responding party's diligence."[137]

In some cases, where no deficiency by the responding party was shown, courts have refused to grant requesting parties access to nonresponsive documents in the training or validation sets to assess the efficacy of the responding party's TAR process.[138]

In *In re Biomet*, the court denied the plaintiffs' request for production of the entire seed set used to train the TAR algorithm.[139] The court observed, "[t]hat request reaches well beyond the scope of any permissible discovery by seeking irrelevant or privileged documents used to tell the algorithm what

---

134. *Id*.

135. Edwards v. Scripps Media, Inc. 331 F.R.D. 116, 117–20 (E.D. Mich. 2019).

136. *Id*. at 120.

137. *Id*. at 125.

138. These cases involved TAR 1.0 procedures, where the training sets tend to be a more discreet subset of the overall TAR population. *See* Section II.B.

139. *In re* Biomet M2a Magnum Hip Implant Prods. Liab. Litig., No. 3:12-MD-2391, 2013 WL 1729682 (N.D. Ind. Apr. 18, 2013); *In re Biomet*, 2013 WL 6405156 (N.D. Ind. Aug. 21, 2013).

not to find."[140] The court reasoned that Federal Rule of Civil Procedure 26(b)(1) only makes relevant, nonprivileged information discoverable, and it commented that "I'm puzzled as to the authority behind [plaintiffs'] request."[141] The court also stated that although The Sedona Principles and local discovery rules encourage parties to cooperate in discovery, neither "expands a federal district court's powers."[142] Accordingly, the court stated, the plaintiffs "can't provide me with [the] authority to compel discovery of information not made discoverable by the Federal Rules."[143]

Similarly, in *Aurora Cooperative Elevator*, the court denied the plaintiff's request to require the defendant to disclose the nonrelevant documents within the training set.[144] Citing Rule 26(b)(1), the court found the defendant's argument was "supported by the language, if not the spirit, of the civil discovery rules," and that "the rules do not authorize ordering the defendants to disclose irrelevant information."[145]

C. Disclosure Required to Address Production Deficiencies

Courts have ordered disclosure of process and documents when a deficiency is shown in the responding party's production or TAR process. Courts have held that reasonableness, rather than perfection, is the standard in discovery, and particularly in document review. Courts may order disclosure of nonresponsive documents where some degree of human error

140. *In re Biomet*, 2013 WL 6405156, at *1.

141. *Id.* at *1–2.

142. *Id.* at *2.

143. *Id.*

144. Aurora Coop. Elevator Co. v. Aventine Renewable Energy-Aurora W. LLC, No. 4:12CV230, 2015 WL 10550240, at *2 (D. Neb. Jan. 6, 2015).

145. *Id*.

is established, even if TAR processes are not considered demonstrably deficient overall. However, errors in a small subset of documents will not generally imply production-wide deficiencies or prompt additional disclosures.

Even where a TAR process was overall reasonable and not deficient, some additional disclosure may be appropriate if specific deficiencies are known. In *Winfield v. City of New York*, the court ordered the City to provide plaintiffs with sample sets of nonprivileged, nonresponsive documents that had been used to train the TAR software.[146] The plaintiffs objected to the City's use of TAR because they believed that the City's reviewers had overdesignated documents as nonresponsive during the training stages and had improperly trained the TAR software.[147] While the court did not find that the TAR process as a whole was defective, it nevertheless found that there was sufficient evidence to justify the plaintiffs' request.[148] The court reasoned "that the sample sets will increase transparency, a request that is not unreasonable in light of the volume of documents collected from the custodians, the low responsiveness rates of documents pulled for review by the TAR software, and the examples that [p]laintiffs have presented, which suggest there may have been some human error in categorization that may have led to gaps in the City's production."[149] Despite its order, the

146. Winfield v. City of New York, No. 15-CV-05236 (LTS) (KHP), 2017 WL 5664852 (S.D.N.Y. Nov. 27, 2017).

147. *See id.* at *12.

148. *See id.* at *25.

149. *Id.* at *9, 11. The court reasoned that responding parties are in the best position to manage their own discovery and are not held to a standard of perfection, noting that courts should not "insert themselves as super-managers of the parties' internal review processes, including training of TAR software, or . . . permit discovery about such process, in the absence of evidence of good cause . . . ."

court acknowledged that "[p]laintiffs have [not] identified anything in the TAR process itself that is inherently defective."[150]

A court may also order disclosure of information about the TAR process where a responding party both fails to provide transparency about its TAR process and where at least some indicia of possible production deficiencies exist. In *In re Broiler Chicken II*, the plaintiffs and a third-party respondent had negotiated and agreed upon search terms. After receiving the third party's production and then discovering TAR had been used, the plaintiffs moved to compel all documents that hit on the negotiated search terms.[151] The court noted the third party was not bound by any court order regarding its review and production process, and it had reserved the right to review documents prior to production in its agreement with the plaintiffs.[152] However, it also acknowledged that the plaintiffs had legitimate questions about the use of TAR given potential "gaps in the production and legitimate questions about what was and was not produced;" for example, the third party had produced a low number of emails compared to the defendants' production, which contained many more emails involving the third party. The court denied the requested relief, but it ordered the third party "to explain its culling method and to justify why documents were not produced based on those agreed upon search terms."[153]

At least one court has granted "discovery about discovery" through a Rule 30(b)(6) deposition where the parties had previously agreed to such an examination. In *In re Santa Fe National*

---

150. *Id*. at 11.

151. *In re* Broiler Chicken II, No. 6:20-2977-RJS-CMR, 2022 WL 2812679 (E.D. Okla. Feb. 7, 2022).

152. *Id*. at *3.

153. *Id*. at *3.

Tobacco Co. Marketing & Sales Practices & Products Liability Litigation, the plaintiffs sought a Rule 30(b)(6) deposition to determine "why the [d]efendants' use of predictive coding failed to produce hundreds of thousands of potentially responsive documents."[154] The plaintiffs also contended that the defendants' use of TAR violated the ESI Order because they did not alert the plaintiffs that they were using it.[155] The court did not rule on whether the use of TAR violated the ESI Order but agreed that "[a]s a result of a predictive-coding issue, the [d]efendants did not produce all relevant, non-privileged discovery."[156] The plaintiffs initially requested the deposition at a status conference on the TAR deficiencies, and the defendants agreed to it at that time.[157] The court thus enforced that agreement and allowed the plaintiffs to take one three-hour 30(b)(6) deposition to "inquire into the defendants' discovery methodology."[158]

D. Disclosure Required to Address Misconduct

A court may require disclosure of training documents as a remedy where the responding party has repeatedly failed to implement an effective TAR process or otherwise engaged in misconduct. In *Independent Living Center v. City of Los Angeles*, the court ordered the use of TAR to search more than two million documents after "little or no discovery was completed" before the discovery cutoff, and the parties had ongoing disputes after "months of haggling" over search terms that yielded large

154. *In re* Santa Fe Nat. Tobacco Co. Mktg. & Sales Practs. & Prods. Liab. Litig., No. MD 16-2695 JB/LF, 2018 WL 3972909, at *1 (D.N.M. Aug. 18, 2018).

155. *Id*. at *2.

156. *Id*. at *11.

157. *Id*. at *4.

158. *Id*. at *11.

numbers of documents for review.[159] Although the defendant was initially concerned about the costs of using TAR, it agreed to do so when the court stated that it would only be required to produce the top 10,000 documents identified by the TAR tool. At the defendant's request, and to avoid subsequent disputes, the court also ordered that the plaintiff "be involved in and play an active role" in the training process, including making "relevance determinations" in the training documents.[160] The court held that the defendant was not necessarily required to engage in a quality-assurance process as part of the TAR protocol; however, if the plaintiff insisted on such a process, then the plaintiff would have to pay for 50 percent of its costs.[161]

E. Failure to Disclose TAR Not Contemplated by ESI Protocol

In *Progressive Casualty Insurance Co. v. Delaney* and *In re Valsartan, Losartan & Irbesartan Products Liability Litigation*, the responding parties had agreed to ESI protocols, which were approved and entered as orders by the courts at the outset of discovery, providing for the use of traditional search terms and manual review. When the review became cost-prohibitive, however, the responding parties unilaterally decided to change course and use TAR without seeking the requesting party's agreement or leave of the court to amend the ESI Order.[162] The court in *Progressive* denied the responding party's request to use

159. Indep. Living Ctr. v. City of Los Angeles, No. 2:12-cv-00551, Minute Order at 1, ECF 375 (C.D. Cal. June 26, 2014).

160. *Id*.

161. *Id*.

162. *In re* Valsartan, Losartan, & Irbesartan Prods. Liab. Litig., 337 F.R.D. 610, 614 (D.N.J. 2020), also discussed in Sections III.B, III.C, V.A, and VI.A; Progressive Cas. Ins. Co. v. Delaney, No. 2:11-cv-00678-LRH-PAS, 2014 WL 3563467, at *2 (D. Nev. Jul. 18, 2014).

TAR and ordered it to produce all documents that hit on the search terms, subject to clawback of privileged documents or the application of privilege filters to withhold documents deemed more likely privileged and identified on a privilege log.[163] The court in *Valsartan* refused to "endorse a TAR protocol that was unilaterally adopted by a producing party without any input from the requesting party."[164] Instead, the court ordered the responding party to use a TAR protocol that was negotiated in part but had not been fully agreed upon by the parties.[165]

In *Valsartan*, the court ordered the production of a sample of 5,000 null-set documents of the plaintiff's choosing in response to the defendant's failure to timely disclose its use of TAR. The defendant first raised its intention to use TAR to cull documents over a year after the court had entered a stipulated ESI Order relating to searching that required timely disclosure if TAR would be used to cull documents. The parties negotiated and almost agreed on a TAR protocol, but the defendant would not agree to submit the protocol for the court to order, or to disclose a sample of 5,000 documents that TAR predicted were not responsive and were withheld from production. Although the defendant then represented to the court that it was abandoning TAR, it nevertheless used TAR and then sought permission to end its review of documents predicted by TAR as not responsive, based on proportionality considerations.

Noting that defendant had violated the ESI protocol "by not timely disclosing its use or possible use of its CMML [TAR 2.0]," the court entered the TAR protocol to which the defendants had previously objected as a court order, giving the plaintiffs the "right to review at the end of [defendant's] production 5,000

163. *Progressive*, 2014 WL 3563467, at *11.

164. *In re Valsartan*, 337 F.R.D. at 622.

165. *Id.* at 624.

alleged nonresponsive documents."[166] *Valsartan* demonstrates that parties should carefully follow provisions of ESI protocols.[167]

166. *Id*. at 617, 624.

167. *See* Section VI regarding ESI protocols.

V. TAR WORKFLOW CONSIDERATIONS

Some issues discussed in the *First Edition Primer* have seen no judicial activity since its publication in 2017 (e.g., retraining the TAR Tool),[168] while others such as keyword culling before TAR and recall thresholds and validation have had multiple decisions.

A. Search-Term Culling Before TAR

Numerous cases have addressed the use of search terms to cull the document population before applying TAR. As illustrated below, there is a split in authority on whether the application of TAR after keyword culling is permissible.

1. Cases Allowing TAR after Keyword Culling

In *In re Biomet*, the court upheld the defendant's use of keywords to cull the collected dataset before applying TAR.[169] The defendant had used keywords to cull the collected document set from 19.5 million documents and attachments down to 3.9 million documents and attachments. After de-duplicating the documents, the defendant used TAR on this smaller data set, identifying almost two million documents for production. The court

168. For example, Smilovits v. First Solar Inc., No. 2:12-cv-00555, slip op. at 1–2, ECF 248 (D. Ariz. Nov. 20, 2014) addressed whether the responding party can be required to respond to additional document requests after it has already used TAR to respond to a prior round of requests. The court held that the defendants' use of TAR in response to the plaintiffs' first round of document requests did not confine the plaintiffs' document discovery to the first round of requests. The court also noted that the defendants had not explained why the search for additional documents required the use of TAR, nor had they provided any concrete information about the costs to "retrain" the TAR tool to deal with subsequent requests.

169. *In re* Biomet M2a Magnum Hip Implant Prods. Liab. Litig., No. 3:12-MD-2391, 2013 WL 1729682 (N.D. Ind. Apr. 18, 2013).

denied the plaintiffs' motion to require the defendant to redo its search and review process using TAR on the entire document population that it had collected, instead of just on the documents that resulted from a keyword search.[170]

The plaintiffs argued that keyword search is less accurate than TAR and that the defendant's efforts were tainted by using keyword search before TAR. The court, however, stated that "[t]he issue before me today isn't whether predictive coding is a better way of doing things than keyword searching prior to predictive coding." Rather, "I must decide whether Biomet's procedure satisfies its discovery obligations[.]"[171]

The court rejected the plaintiffs' arguments, holding that the defendant's methodology satisfied the standard set forth in Federal Rules of Civil Procedure 26 and 34, namely, that its efforts must be "reasonable." The court also considered proportionality factors in its decision:

> It might well be that predictive coding, instead of a keyword search . . . would unearth additional relevant documents. But it would cost Biomet a million, or millions, of dollars to test the [plaintiffs'] theory that predictive coding would produce a significantly greater number of relevant documents. Even in light of the needs of the hundreds of plaintiffs in this case, the very large amount in controversy, the parties' resources, the importance of the issues at stake, and the importance of this discovery in resolving the issues, I can't find that the likely benefits of the discovery proposed by [plaintiffs] equals or outweighs its

170. *Id.* at *2.

171. *Id*.

> additional burden on, and additional expense to, Biomet.[172]

In *Rio Tinto*, the court permitted the use of keyword culling before TAR because it was agreed to as part of the parties' stipulated protocol.[173] "The Court itself felt bound by the parties' protocol, such as to allow keyword culling before running TAR, even though such pre-culling should not occur in a perfect world." But the court also noted that "the standard for TAR is not perfection," nor "best practices," "but rather what is reasonable and proportional under the circumstances."[174]

In *Bridgestone*, after an initial search-term cull done according to a stipulated court order, the court permitted the responding party to "switch horses in midstream" to undertake a hybrid approach, using TAR on the resulting document set of more than two million documents requiring review.[175] The court expressly recognized that TAR use was a "judgment call" and raised the option that the requesting party could also consider switching to TAR if it believed that would be more efficient for its own review.[176]

Several recent decisions suggest a growing trend that courts find keyword culling prior to the use of TAR to be permissible. In *Livingston*, the court permitted the defendant to use TAR to review the culled document set over the plaintiffs' objection that

---

172. *Id.* at *3.

173. Rio Tinto PLC v. Vale S.A., No. 14 Civ. 3042(RMB)(AJP), 2015 WL 4367250, at *1 (S.D.N.Y. July 15, 2015).

174. *See id*.

175. Bridgestone Ams., Inc. v. Int'l Bus. Machs. Corp., No. 3:13-1196, 2014 WL 4923014, at *1 (M.D. Tenn. July 22, 2014).

176. *Id. See also* United States *ex rel.* Proctor v. Safeway, Inc., No. 11-cv-3406, 2018 WL 1210965, at *3 (C.D. Ill. Mar. 8, 2018) (while not specifically evaluating the issue, the court did not object to party's TAR to conduct its responsiveness review on the dataset collected using search terms).

the review would create an incomplete production.[177] The court noted that application of the TAR tool to the original collection of documents would be unduly burdensome and wasteful. In its ruling, the court agreed with the defendant that it was using TAR as a responsiveness review tool and not a culling tool, and accordingly, it could be used after application of agreed upon search terms because "it satisfies the reasonable inquiry standard and is proportional to the needs of this case under the federal rules."[178]

In *Valsartan*, while holding that the defendant's use of TAR after using negotiated search terms to cull the data for review and without notification to the plaintiffs violated the entered ESI protocol, the court made clear that the lack of notice was the issue, observing "[a]mple case law exists to support [defendants'] position that in appropriate instances layering may be done."[179]

Further, in *Maurer v. Sysco Albany, LLC*, the court upheld the defendant's use of TAR post-search-term culling.[180] The parties had disagreed on the scope of custodians, date ranges, and search terms as well as the defendant's use of TAR post-culling. The plaintiff proposed that the defendant either manually review all documents resulting from a broad list of search terms or use TAR on each custodian's entire mailbox for a date range that covered a large time period. The defendant proposed that it use TAR after application of more narrow date ranges and

177. Livingston v. City of Chicago, No. 16 CV 10156, 2020 WL 5253848, at *1 (N.D. Ill. Sept. 3, 2020). *See also* case discussion in Sections III.C, IV.B, and VI.A.

178. *Id*. at *3.

179. *In re* Valsartan, Losartan, & Irbesartan Prods. Liab. Litig., 337 F.R.D. 610, 615 (D.N.J. 2020). Also discussed in Sections III.B and IV.E and VI.A.

180. Maurer v. Sysco Albany, LLC, No. 1:19-CV-821(TJM/CFH), 2021 WL 2154144 (N.D.N.Y. May 27, 2021).

search terms. In upholding the use of TAR on data resulting from the application of search terms, the court noted that "the cost of conducting a linear review of every hit resulting from a search term-based search that includes all custodians' names and name derivatives or reviewing the full custodian accounts using predictive coding dating back to 2013 is not proportional to the benefit and importance of ESI in resolving the issues presented in this case."[181] The court did, however, order the defendant to modify its search term list used for culling to include certain broader terms proposed by the plaintiff.[182]

In *Huntsman v. Southwest Airlines Co.*, the plaintiff challenged, inter alia, the defendant's use of keyword searches to limit to scope of ESI review.[183] The court rejected the plaintiff's challenge, finding that the defendant's "approach to using keyword searches and technology-assisted review in tandem does not offend the court's expectations that the parties conduct a reasonable inquiry as required by the rules."[184]

In *In re Diisocyanates*, in ruling on several motions to compel regarding search-term culling, TAR, and validation protocols, the court held that a reasonable set of search terms could be used to cull down collected data prior to applying TAR.[185] The court declined, however, to approve either party's proposed search-term lists, sending them back to renegotiate. In so doing, it noted that it is reasonable to use broader search terms to cull data prior to application of TAR because recall is more

181. *Id.* at *9.

182. *Id*.

183. Huntsman v. Sw. Airlines Co., No. 19-cv-00083-PJH, 2021 WL 3504154, at *3 (N.D. Cal. Aug. 10, 2021).

184. *Id*. at *3.

185. *In re* Diisocyanates Antitrust Litig., No. 18-1001, MDL No. 2862, 2021 WL 4295729 (W.D. Pa. Aug. 23, 2021), *adopted by In re Diisocyanates*, 2021 WL 4295719 (W.D. Pa. Sept. 21, 2021).

important than precision in those instances. "In this regard, it should be kept in mind that the function of search terms in this case is not to identify documents for production or even to select those that will be provided directly to human reviewers; it is to narrow the universe of documents to which TAR will be applied. In this context, precision, which is what defendants appear to seek, is relatively less important than recall."[186]

After keyword searches were complete and the *Diisocyanates* defendants asserted they had completed their TAR review, the special master considered the recall rates of the search terms and TAR processes together, as well as the quantity and quality of each process individually. He also stated that "because large swaths of documents had already been excluded by search terms, it is particularly important not to stop the [TAR 2.0] review of the remaining documents prematurely."[187]

In *Zhulinska v. Niyazov Law Group, P.C.*, the court found the defendant failed to prove unreasonable burden to review additional document volumes associated with the plaintiff's requested keyword searches, in part because "predictive coding is an efficient and acceptable means of culling relevant responsive documents to be produced from ESI identified through keyword searches."[188]

Lastly, in *In re Broiler Chicken II*, the court held that a third party had not been required to seek approval from the court to use TAR in addition to negotiated keyword searches, where the third party had "reserved the right to review the documents for

186. *Id.* at *10. Recall and precision are discussed in Section V.C.

187. *In re Diisocyanates*, 2022 WL 17668470, at *12 (W.D. Pa. Oct. 19, 2022), *modified by In re Diisocyanates*, ECF No. 800 (W.D. Pa. Oct. 21, 2022).

188. Zhulinska v. Niyazov Law Grp., P.C., No. 21-CV-1348, Memorandum and Order at 8, ECF 58 (E.D.N.Y. Nov. 12, 2021).

relevance" in negotiations about keywords.[189] However, given concerns about potential "gaps in the production," the court ordered the third party to disclose its TAR methodology to the requesting party.[190]

2. Cases Not Allowing TAR after Keyword Culling

While some courts have allowed TAR after keyword culling, others have disallowed it. In *FCA U.S. v. Cummins*, the court held that TAR should be applied before culling the document set with search terms.[191] As the court explained, "[a]pplying TAR to the universe of electronic material before any keyword search reduces the universe of electronic material is the preferred method. The TAR results can then be culled by the use of search terms or other methods."[192]

In *In re Allergan Biocell Textured Breast Implant Products Liability Litigation*, the defendants sought to use TAR after search terms had been applied, citing burden and efficiency concerns.[193] The defendants also argued that that the application of search terms prior to TAR was "consistent with the majority of courts" that had addressed the issue.[194] The court disagreed

189. *In re* Broiler Chicken II, No. 6:20-2977-RJS-CMR, 2022 WL 2812679, at *2 (E.D. Okla. Feb. 7, 2022).

190. *Id.* at *3. *See also* Klein v. Facebook, Inc., 2021 U.S.Dist. LEXIS 175738, *8 (N.D.Cal. 2021) (requiring responding party to disclose its intent to use TAR and how it will be used in conjunction with search terms, but not requiring a party using TAR to follow or negotiate any particular protocol).

191. FCA US LLC v. Cummins Inc., No. 16-12883, 2017 WL 2806896 (E.D. Mich. Mar. 28, 2017).

192. *Id.* at *1.

193. *In re* Allergan Biocell Textured Breast Implant Prods. Liab. Litig., No. 2:19-md-2921 (BRM)(ESK), 2022 WL 16630821, at *1 (D.N.J. Oct. 25, 2022).

194. *Id.* at *2.

with the defendants' "characterization of the case law," noting that "[t]here is no such general principle espoused by the courts or the commentators."[195] In finding that the defendants could not use TAR after search terms, the court emphasized the defendants had not sufficiently established the burden, and that the court-ordered ESI Protocol stipulated by the parties required them to cooperate, but they had not reached agreement on TAR.[196]

The court in *Progressive* also considered the court's ESI order.[197] The court denied the plaintiff's request, which it made late in the discovery process and without agreement from defendant, to switch from the search terms and manual review process provided for in the court's ESI order to search-term culling followed by TAR. The court reasoned that the plaintiff's proposal violated the parties' stipulated ESI protocol, as entered by the court, which had been contentiously negotiated by the parties. Further, the court criticized the plaintiff's plan to apply TAR only to documents hitting the search terms, observing that its proposed process "lacks transparency and cooperation regarding the search methodologies [to be] applied" and would therefore be inconsistent with the "best practices" guide of its own TAR vendor.[198]

B. Validation

Some courts have held that when a party uses TAR, the Federal Rule of Civil Procedure 26(g) "reasonable inquiry" standard incorporates an obligation for the responding party to

195. *Id*.

196. *Id*. at *4.

197. Progressive Cas. Ins. Co. v. Delaney, No. 2:11-cv-00678-LRH-PAL, 2014 WL 3563467 (D. Nev. July 18, 2014). Section VI discusses protocols.

198. *Id*. at *10.

validate its results.[199] Courts may require validation regardless of whether parties use TAR or keyword searches. *City of Rockford v. Mallinckrodt ARD Inc.* involved a responding party that had refused to validate the results of its keyword searches. While the parties had agreed to use of keyword searches, they approached the court at an impasse on post-production validation processes.[200] The plaintiffs proposed that the defendants provide a random sample of the null set, followed by meeting and conferring to determine whether any additional terms or term modifications were necessary. The court agreed, reasoning that "random sampl[ing] of the null set is a part of the TAR process" to quantify "the documents that will be missed and not produced," and there is "no reason . . . that a random sampling of the null set cannot be done when using key word searching."[201] The court adopted the parties' proposed ESI order "with the inclusion of Plaintiffs' proposal that a random sample of the null set will occur after the production and that any responsive documents found as a result of that process will be produced."[202]

In one early TAR case, *Independent Living Center v. City of Los Angeles*, after the parties disagreed whether the TAR advisor had said "quality control" (validation) was needed, the court

---

199. *In re* Diisocyanates Antitrust Litig., No. 18-1001, MDL No. 2862, 2021 WL 4295729 at *6 (W.D. Pa. Aug. 23, 2021), *adopted by In re Diisocyanates*, 2021 WL 4295719 (W.D. Pa. Sept. 21, 2021).

200. City of Rockford v. Mallinckrodt ARD Inc., 326 F.R.D. 489 (N.D. Ill. 2018).

201. *Id*. at 493, 494.

202. *Id*. at 496. *But see* Jim Hawk Truck-Trailers of Sioux Falls, Inc. v. Crossroad Trailer Sales & Serv. Inc., No. 4:20-CV-04058-KES, 2022 WL 3010143, at *7 (D.S.D. July 29, 2022) (considering only relevancy rate of last 2,000 documents reviewed in TAR 2.0 workflow, among other factors, to determine further review would not be proportional).

held that if the requesting party wanted validation done, it would have to share costs for that process.[203]

Beyond the threshold question of whether a party must validate, opinions focus on the validation metrics of recall and precision. When using TAR to find responsive documents, "recall" is a metric that represents an estimate of the percentage of responsive documents that are found out of the entire set of responsive documents in the TAR document set.[204] "Precision" represents an estimate of the percentage of documents that are truly responsive out of the set of documents identified as potentially responsive.[205]

1. Role of Recall

Generally, recall metrics receive more attention from parties than precision metrics. In *Lawson v. Spirit AeroSystems*, the defendant used TAR to produce with a recall of approximately 85

---

203. Indep. Living Ctr. v. City of Los Angeles, No. 2:12-cv-00551, Minute Order at 3, ECF 375 (C.D. Cal. June 26, 2014) ("It is a feature available in predictive coding which quantifies the level of accuracy in the search. The fact that it exists in the system does not mean that the City has to employ it and pay for it").

204. "When describing search results, recall is the number of documents retrieved from a search divided by all of the responsive documents in a collection. For example, in a search for documents relevant to a document request, it is the percentage of documents returned compared against all documents that should have been returned and exist in the data set." *The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition*, 21 SEDONA CONF. J. 263, 360–61 (2020) (citing The Sedona Conference, *Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, 15 SEDONA CONF. J. 217 (2014).

205. "When describing search results, precision is the number of true positives retrieved from a search divided by the total number of results returned. For example, in a search for documents relevant to a document request, it is the percentage of documents returned that are actually relevant to the request." *Id.* at 354.

percent, which the court confirmed was reasonable and within a typical range for TAR matters.[206] The plaintiff had demanded that the defendant switch from keyword searching to a TAR methodology, which the defendant ultimately agreed to do, subject to filing a motion to shift costs based on proportionality.[207] An initial review using TAR 2.0 achieved a 68.5 percent recall rate of responsive documents, but the plaintiff insisted that the process be repeated until a 75 to 85 percent recall rate was achieved. The defendant agreed to 80 percent recall and then, after stopping its review, determined that it had reached 85 percent recall.[208]

Even then, however, the plaintiff moved to compel the defendant to perform a second-level review of the set of residual TAR documents: 1,850 potentially responsive TAR documents that were reviewed in first-level review, but not in the second-level review, once the desired recall rate was reached.[209]

The court denied the motion, explaining that the defendant's TAR review process was reasonable, and that the plaintiff's request for additional review was disproportionate to the needs of the case.[210] The court noted that at an expense of $600,000, only 3.3 percent of the 322,000-document set was found to be responsive, and the defendant produced 85 percent of those responsive documents.[211] The court rejected the perfection that the

---

206. Lawson v. Spirit AeroSystems, Inc., No. 18-1100-EFM-ADM, 2020 WL 1813395 (D. Kan. April 9, 2020). *See also Lawson*, 2020 WL 3288058 (D. Kan. Jun. 18, 2020), *aff'd*, 2020 WL 6939752 (D. Kan. Nov. 24, 2020), and Sections III.C and VIII.B.

207. *Lawson,* 2020 WL 1813395, at *4; *see also Lawson*, 2020 WL 3288058, at *6.

208. *Lawson,* 2020 WL 1813395, at *7–8.

209. *Id*. at *5.

210. *Id*. at *8.

211. *Id*. at *16.

plaintiff "effectively demand[ed], which is a 100 percent target recall rate."[212] Ultimately, the plaintiff had to pay for its unreasonable demands when the court approved fee shifting of the defendant's TAR costs to the plaintiff, as discussed below.[213]

In *In re Diisocyanates*, the parties proffered dueling proposals on the use of certain search terms and specific TAR methodologies.[214] The court-appointed special master found that due to the complexities of TAR, Rule 26(g)'s reasonable inquiry requirement requires the responding party to validate its TAR methodology.[215] After examining the plaintiffs' and the defendants' proposed TAR methodologies, the special master concluded that the defendants' proposed methodology contained serious flaws that would preclude them from certifying that their discovery responses were reasonable under Rule 26(g).[216] Among other matters, the defendants proposed to calculate estimated recall based on elusion sampling[217] of the unseen TAR collection and did not include documents that failed to hit on search terms, which may have resulted in an overestimation of the recall rate.[218] The special master held, "In the absence of [an agreement providing otherwise], it would be plainly unreasonable to

212. *Id*. at *9.

213. *See id*.

214. *In re* Diisocyanates Antitrust Litig., No. MC 18-1001, MDL No. 2862, 2021 WL 4295729 (W.D. Pa. Aug. 23, 2021), *adopted by In re Diisocyanates*, 2021 WL 4295719 (W.D. Pa. Sept. 21, 2021).

215. *In re Diisocyanates*, 2021 WL 4295729 at *6 (W.D. Pa. Aug. 23, 2021).

216. *Id*. at *9.

217. Elusion is "[t]he percentage of documents of a search's null set that were missed by the search, usually determined with review of a random sample of the null set." *The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition*, 21 SEDONA CONF. J. 263, 304 (2020). Elusion was used to estimate recall in *Diisocyanates*.

218. *In re Diisocyanates*, 2021 WL 4295729, at *9.

calculate estimated recall for the TAR portion of the process alone."[219]

The *Diisocyanates* defendants then used keyword searches and a TAR 2.0 review workflow, resulting in recall rates from both processes that ranged from 74 to 89 percent, which the special master held was reasonable and met the 70 to 80 percent range the parties had represented as generally acceptable.[220] The special master's analysis included not only quantitative recall considerations, but also qualitative analysis of keyword and TAR validation sets, which were samples of documents not found by those workflows.[221] The qualitative analysis generally supported a conclusion that, on their own, any remaining responsive documents were insufficiently valuable to justify further search or review because they were similar to documents that were found.[222] The validation process did not require rereviewing the accuracy of a sample of the already-reviewed documents.[223]

Some defendants were nevertheless required to continue review based on their last batches before stopping the review, which were 19 percent and 15 percent relevant. The special

---

219. *Id*.

220. *In re Diisocyanates*, 2022 WL 17668470, *11, 18 (W.D. Pa. Oct. 19, 2022), *modified by In re Diisocyanates*, ECF No. 800 (W.D. Pa. Oct. 21, 2022).

221. *Id*, at *4–7. The special master also recognized limitations of recall when analyzing reasonability of a search process. *Id*. at 6 ("At the same time, broad validation statistics such as recall, standing alone, are of limited utility in ascertaining whether a party has done a reasonable job of searching for such rare documents.").

222. *Id*. at *4–7.

223. *Id*. at *8 ("The defendants' methodology may be imperfect, and it may result in higher estimated recall figures than if the plaintiffs' approach were used, but it is not unreasonable, particularly given the extent by which the defendants exceeded the lower end of the acceptable range").

master instructed the parties to continue their review at least until relevance declined to 10 percent and the responsive documents in the last-reviewed batches were insufficiently valuable, based on proportionality factors.[224]

2. Role of Precision

While recall metrics tend to have some established range of acceptability when using TAR, acceptable precision metrics that correspond to those recall points can vary widely from case to case. While cases dealing in these metrics focus on how low recall may reasonably be, one case deals in the opposite issue: how low precision may reasonably be (despite involving higher recall). In *In re Domestic Airline Travel Antitrust Litigation*, a multidistrict class action, the parties had entered into a validation protocol "to ensure accuracy and completeness."[225] One business day before the production deadline, the defendant provided erroneous TAR validation metrics to the plaintiffs, reporting an estimated recall of 85 percent and an estimated precision of 58 percent. The defendant also provided the validation sampling metrics required by the TAR protocol. "When Plaintiffs analyzed the metrics, they found that the statistics from the validation sample indicated that the TAR process resulted in a recall of 97.4% and precision of 16.7%," in contrast to the metrics provided by defendant.[226] After exchanges between the parties, the defendant acknowledged that it had made an error.[227] The court stated that "the answer seems to be that unless

224. *Id*. *See* Section VII, discussing the proportionality analysis.

225. *In re* Domestic Airline Travel Antitrust Litig., No. 15-1404 (CKK), 2018 WL 4441507, at *3 (D.D.C. Sept. 13, 2018).

226. *Id.* at *4.

227. *Id*.

[defendant] starts the process over, Plaintiffs must review all the documents."[228]

In granting the plaintiffs' motions to extend fact discovery, the court noted that "[defendant's] production of core documents . . . varied greatly from the control set in terms of the applicable standards for recall and precision and included a much larger number of non-responsive documents that [sic] was anticipated. Additionally, Plaintiffs diligently sought an amendment of the schedule after it became apparent that there was no way to resolve the excess non-responsive document issue short of starting over, and the 70 attorneys engaged in document review were not going to be able to complete the job under the current deadlines."[229]

228. *Id*.

229. *Id*. at *7.

VI. DEFERENCE TO COURT-ORDERED ESI PROTOCOLS

As ESI protocols have become increasingly routine, courts have assessed a responding party's production decisions against any governing protocol, often enforcing the provisions negotiated by the parties or imposed by the court.[230] Where no ESI protocol exists, however, the outcome is more varied.

In *Livingston* and *Valsartan*, the existence of a negotiated and entered ESI protocol dictated how the court handled a party's decision to use TAR.

In *Livingston*, the court ruled that the defendant's use of TAR was permissible because it did not contradict the existing protocol ordered by the court.[231] In that case, the parties had spent two years negotiating an ESI protocol, which was silent on the method and process for review but included a detailed process for collection and keyword culling. After the court entered the protocol, the defendant notified the plaintiffs that it intended to use TAR to review the keyword-culled documents. The plaintiffs objected, arguing that because the defendant never mentioned using TAR during the protocol negotiations, doing so would violate the protocol. The court disagreed, noting that the protocol "did not set forth the review methodology that the City must use to identify responsive ESI."[232]

---

230. *See also* Section V.A on use of TAR after search-term culling.

231. Livingston v. City of Chicago, No. 16 CV 10156, 2020 WL 5253848 (N.D. Ill. Sept. 3, 2020). *See also* case discussion in Sections III.C, IV.B, and V.A.

232. *Id.* at *3; *see also id.*, citing *The Sedona Principles, Third Edition*, *supra* note 3, Principle 6 (citing Sedona Principle 6, court held that the defendant could use TAR to review the culled documents because "Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own [ESI].").

In contrast, the court in *Valsartan* ruled that the defendant violated the existing ESI protocol when it did not timely disclose that it would use TAR to cull documents without the plaintiffs' consent, because the protocol required timely disclosure when its use was reasonably foreseeable.[233] In ruling that the defendant violated the protocol, however, the court nevertheless noted that it "agree[d] with the line of cases that holds that a producing party has the right in the first instance to decide how it will produce its documents."[234]

Whether parties unilaterally design their own TAR protocol or enter into one by agreement or court order, it is important to understand what such protocols require and how those requirements may be treated by the Court. In *Domestic Airline*, for example, the parties entered into a validation protocol "to ensure accuracy and completeness."[235] That agreement was later used to support the plaintiffs' successful request for an extension of fact discovery where the defendant's production demonstrated a low level of precision, resulting in the production of "millions of non-responsive documents."[236] The protocol required the defendant to "set a minimum estimated recall rate of 75% but [to] endeavor to achieve a higher estimated recall rate if that rate may be obtained with a reasonable level of precision through reasonable additional training effort."[237] In granting the plaintiffs' extension request, the court reasoned that the TAR

233. *In re* Valsartan, Losartan, & Irbesartan Prods. Liab. Litig., 337 F.R.D. 610, 617 (D.N.J. 2020). This case is also discussed in Sections III.B., III.C, IV.E., and V.A.

234. *Id.* at 616, citing Hyles v. New York City, 10 Civ. 3119 (AT)(AJP), 2016 WL 4077114, at *2 (S.D.N.Y. Aug. 1, 2016).

235. *In re* Domestic Airline Travel Antitrust Litig., No. 15-1404 (CKK), 2018 WL 4441507, at *3 (D.D.C. Sept. 13, 2018).

236. *Id.* at *4.

237. *Id.* Recall and precision are discussed in Section V.C.

protocol noted that a reasonable level of precision was a concern, contradicting the defendant's argument that the plaintiffs wanted a high level of TAR recall "without focusing on precision" and "got what they bargained for."[238]

Courts have reached differing conclusions on whether a responding party may switch to TAR in the middle of discovery after having previously agreed to use search terms and manual review.

In *Progressive*,[239] the court denied the plaintiff's request to use TAR. The factors the court cited included: the plaintiff sought to use TAR extremely late in the discovery period; it had not yet produced a single document; it had previously agreed in the parties' ESI protocol to use search terms and manual review; it was not willing to reveal its coding decisions and irrelevant documents in the seed and later training sets; and it made the decision to switch to TAR unilaterally, without informing the defendants or the court.[240] According to the court, the parties had "spent months narrowing search terms," at the plaintiff's insistence, to reduce its burden.[241] The narrowed search terms that the parties agreed on yielded 565,000 "hit" documents out of a total population of 1.8 million. Although the plaintiff had initially represented that it would begin production in September 2013 and complete it by the end of October 2013, it advised the requesting party on December 20, 2013, that the process of

238. *Id.* at *5. See also Youngevity Int'l Corp. v. Smith, No. 16-cv-00704-BTM (JLB), 2017 WL 6541106, at *1, *12 (S.D. Cal. Dec. 21, 2017) (raising fee-shifting option for requesting party to conduct TAR on "document dump" where responding party produced all results of keyword searches without doing any relevance review to remove nonresponsive documents).

239. Progressive Cas. Ins. Co. v. Delaney, No. 2:11-cv-00678-LRH-PAL, 2014 WL 3563467 (D. Nev. July 18, 2014).

240. *Id.* at *8–10.

241. *Id.* at *5.

reviewing the documents retrieved by the search terms was unworkable.[242]

As an alternative to manual review, the plaintiff proposed to apply TAR to the 565,000 documents that "hit" on the search terms and estimated that plaintiff's TAR process would result in a recall of 70 to 80 percent (i.e., that it would find 70 to 80 percent of the total number of relevant documents in the collection). The plaintiff would then manually review the documents identified by TAR for production.[243]

The *Progressive* court rejected the plaintiff's proposal on the grounds that it had previously agreed to manually review the search term hits and it was too late to change course, particularly since its proposal lacked transparency and cooperation and would further delay completion of discovery. The court indicated, however, "[h]ad the parties worked with their e-discovery consultants and agreed at the onset of this case to a predictive coding-based ESI protocol, the court would not hesitate to approve a transparent, mutually agreed upon ESI protocol."[244]

Similarly, in *In re Allergan Biocell*, the court considered the parties' ESI protocols in denying the defendant's request to apply TAR after the application of search terms.[245] The court noted that the ESI protocols addressed the use of search filtering technology and required the parties to confer and agree upon the application of any such technology, including TAR.

---

242. *Id.* at *4–5.

243. *See id*.

244. *Id.* at *9.

245. *In re* Allergan Biocell Textured Breast Implant Prods. Liab. Litig., No. 2:19-md-2921 (BRM)(ESK), 2022 WL 16630821, at *1 (D.N.J. Oct. 25, 2022).

In *Bridgestone*,[246] in contrast, the court permitted the plaintiff to change its search-and-review methodology to TAR mid-stream, based on the plaintiff's determination that it would be a much more efficient process, despite the defendant's objections that the request was an "unwarranted change in the original case management order," and that it would be unfair to allow the use of TAR "after an initial screening has been done with search terms."[247] In permitting the plaintiff "to switch horses in midstream," the court observed "the use[] of predictive coding is a judgment call, hopefully keeping in mind the exhortation of Rule 26 that discovery be tailored by the court to be as efficient and cost-effective as possible." The court noted that the case involved "millions of documents to be reviewed with costs likewise in the millions."[248]

246. Bridgestone Ams., Inc. v. Int'l Bus. Machs. Corp., No. 3:13-1196, 2014 WL 4923014 (M.D. Tenn. July 22, 2014).

247. *See id.* at *1.

248. *Id*.

VII. PROPORTIONALITY

Courts may weigh proportionality factors in assessing whether a responding party employing TAR has discharged its discovery obligations. For example, in *Davine v. The Golub Corp.*, the court permitted defendants to use TAR to review documents and "cease their review [once] . . . they made a good faith determination that the burden of continuing the review outweighs the benefit in terms of identifying relevant documents."[249]

In *City of Rockford v. Mallinckrodt*, the court rejected the responding party's argument that reviewing a random sample from the null set to validate the results of the keyword search process would be disproportionate.[250] The court noted that in its experience and understanding, reviewing a random sample of a null set would not be unreasonably expensive or burdensome.[251] The court stated, "[v]alidation and quality assurance are fundamental principles to ESI production. The process provides the reasonable inquiry supporting the certification under Rule 26(g)."[252] The court also stated, "critically, Defendants have failed to provide any evidence to support their contention" that it would be expensive and burdensome.[253]

Although the producing party's argument focused on expense and burden, the court went on to analyze the proportionality factors under Federal Rule of Civil Procedure 26(b)(1). First, the court stated that the issues at stake—having to do with pharmaceuticals pricing—were substantial, having garnered

249. Davine v. Golub Corp., No. 3:14-cv-30136-MGM, 2017 WL 549151, at *1 (D. Mass. Feb. 8, 2017).

250. City of Rockford v. Mallinckrodt ARD Inc., 326 F.R.D. 489 (N.D. Ill. 2018).

251. *See id.* at 495.

252. *Id.* at 494.

253. *Id*. at 495.

national media attention.[254] Second, the court found that the potential amount in controversy was "extraordinary," and "in today's legal vernacular, these are 'bet the company' cases." Third, the defendants had access to the majority of the relevant information in the case. Fourth, "as to resources, the main defendant is a large international pharmaceutical company with substantial resources." Fifth, the court found that the ESI would "play a key role in resolving the issues in these cases." Finally, the court found that "the burden and expense of a random sampling of the null set does not outweigh its likely benefit of ensuring proper and reasonable—not perfect—document disclosure."[255] Accordingly, the court ordered defendants to review a random sample of the null set based on a 95 percent confidence level with a margin of error of plus-or-minus 2 percent.[256]

ESI production can still be burdensome even when the producing party uses TAR, so proportionality may be an issue even when TAR is used. In *County of Cook v. Bank of America Corp.*, the district court rejected the plaintiff's argument that the defendants' use of TAR affected the magistrate judge's assessment of the "burdens and [] volume of data" that would result from the searches the plaintiff proposed.[257] The court pointed out that the defendants to date had reviewed 400,000 documents for the 38 court-ordered custodians and had 36 attorneys working full time for three months reviewing documents. Additionally, the

254. *Id*.

255. *Id.* at 495.

256. *See id*. at 496. *Cf.* Jim Hawk Truck-Trailers of Sioux Falls, Inc. v. Crossroad Trailer Sales & Serv. Inc., No. 4:20-CV-04058-KES, 2022 WL 3010143, at *7 (D.S.D. July 29, 2022) (considering only relevancy rate of last 2,000 documents reviewed in TAR 2.0 workflow, among other factors, to determine further review would not be proportional).

257. County of Cook v. Bank of Am. Corp., No. 14 C 2280, 2019 WL 5393997, at *3 (N.D. Ill. Oct. 22, 2019).

defendants' ESI vendor costs were projected to exceed $1.3 million. The court held that "[t]hese numbers undermine any suggestion that Defendants' use of TAR to aid in their ESI production affects [the magistrate judge's] proportionality basis for denying the County's request for ESI from the [additional] custodians at issue here."[258]

In *In re Diisocyanates*, the special master analyzed whether proportionality considerations justified defendants stopping their TAR 2.0 review, with one defendant's last two batches being 15 percent responsive, and the other's was 19 percent. Given that this antitrust matter involved evidence that would be a "mosaic" of circumstantial evidence, the additional relevant documents that TAR continued to find were of sufficient value for the reviews to continue, even if "not entirely novel."[259]

258. *Id*.

259. *In re* Diisocyanates Antitrust Litig., No. 18-1001, 2022 WL 17668470, *12 (W.D. Pa. Oct. 19, 2022), *modified by In re Diisocyanates*, ECF No. 800 (W.D. Pa. Oct. 21, 2022).

VIII. FEE SHIFTING

The committee notes to the 2015 amendments to Rule 26 include a reminder that "a responding party ordinarily bears the costs of responding."[260] However, in some cases involving TAR, courts have ordered cost shifting, and in so doing, paid particular attention to the efficiencies gained from using TAR or the inefficiencies resulting from a party's refusal to adopt or timely propose it.

A. Costs Split Between Parties

In some cases, courts have departed from the general rule and have instead allocated costs of responding among the parties. In *Lawson v. Spirit AeroSystems*, the court granted the defendant's motion to shift the TAR-related costs and allocated the costs 80 percent to the plaintiff and 20 percent to the defendant because the plaintiff had "wanted to proceed with the TAR process at a point in time when it was disproportional to the needs of the case."[261] The parties had engaged in protracted negotiations and motion practice related to discovery, initially involving disputes relating to search terms and the proposed custodians. The plaintiff then insisted that the defendant switch to a TAR methodology and the defendant agreed, subject to filing a motion to shift costs if the effort was considered disproportionate. Throughout the TAR process, the defendant acceded to the plaintiff's continued demands until it took the position, and the court agreed that it was finished. As discussed above, the court

---

260. FED. R. CIV. P. 26 advisory committee's note to 2015 amendment. *See also*, OSI Rest. Partners, LLC v. United Ohana, LLC, No. 12353-CB, 2017 WL 396357, at *2 (Del. Ch. Jan. 27, 2017) (discussed Section III.C), adhering to this principle.

261. Lawson v. Spirit AeroSystems, Inc., No. 18-1100-EFM-ADM, 2020 WL 3288058, at *22 (D. Kan. Jun. 18, 2020), *aff'd*, 2020 WL 6939752 (D. Kan. Nov. 24, 2020). *See also* Sections III.C and V.C for further discussion of this case.

declined to force the defendant to continue its review when its estimated recall met or exceeded even that initially demanded by the plaintiff.[262]

The court found it was appropriate to shift costs of the TAR review to the plaintiff because "Lawson's continued pursuit of the ESI dataset via TAR was not proportional to the needs of the case," and he had pursued "needlessly overbroad discovery."[263] Because Lawson had "wanted to proceed with the TAR process at a point in time when it was disproportional to the needs of the case," the court held that he should bear much of the cost, to protect the defendant.[264]

In *Youngevity International v. Smith*, the parties had agreed to disclose keyword search hit reports.[265] However, the plaintiffs later refused to do so and produced 4.2 million pages of its keyword hits without having reviewed them (and admitted that it further erroneously failed to produce another 700,000 documents). The plaintiffs argued that it had produced the documents exactly as the defendants requested, that every document produced had hit on at least one of the agreed-upon search terms, and that the volume of the production resulted from the defendants' failure to narrow the search terms.[266] The court disagreed, finding that the productions "improperly exceeded" the defendants' requests and did not comply with the parties' agreed-upon protocol.[267] The court gave the plaintiffs two

262. *See Lawson*, 2020 WL 1813395 (D. Kan. Apr. 9, 2020); *In re* Domestic Airline Travel Antitrust Litig., No. 15-1404 (CKK), 2018 WL 4441507, at *3 (D.D.C. Sept. 13, 2018).

263. *Lawson,* 2020 WL 3288058, at *21.

264. *Id*. at *22.

265. Youngevity Int'l Corp. v. Smith, No. 16-cv-00704-BTM (JLB), 2017 WL 6541106, at *1, *12 (S.D. Cal. Dec. 21, 2017).

266. *Id.* at *8.

267. *Id.* at *8.

options: (1) reproduce the documents after reviewing for responsiveness and privilege or (2) produce the 700,000 responsive documents omitted from prior productions without further review and pay the defendants' costs for applying TAR to those documents and documents from prior productions.[268] The court also ordered the plaintiffs to reimburse the defendants for fees and expenses incurred in its motion.[269]

Finally, in *Independent Living Center v. City of Los Angeles*, certain TAR fees were ordered split between the parties.[270] In that case, the court ordered the responding party to use TAR to identify the 10,000 most relevant documents without using previously identified documents as seeds, despite the increased cost to it.[271] However, the court ruled that if the plaintiff wanted any documents beyond the 10,000, it would have to pay 100 percent of the producing party's costs in producing them, including the attorney's fees incurred to review the additional documents.[272]

B. Other Awards of TAR Fees and Expenses

In some matters, courts must determine issues related to TAR fees and expenses, such as payments from funds to counsel in a class action. In other matters, courts must determine whether a particular statute requires the other party to pay for TAR.

One California state court decision shifted TAR-related costs to a requesting party, based on a state procedural rule permitting such allocation. In *Dremak v. Urban Outfitters, Inc.*, the

268. *Id.* at *8.

269. *See id.* at *11–12.

270. Indep. Living Ctr. v. City of Los Angeles, No. 2:12-cv-00551, Minute Order at 1, ECF 371 (C.D. Cal. June 13, 2014).

271. *Id.*

272. *Id.*

California Court of Appeal affirmed a trial court's post-judgment award to defendants, who prevailed in the case, of $57,912.84 of costs associated with their production of documents in response to the plaintiffs' discovery requests, which included the use of TAR.[273] Under California law, the trial court had discretion to grant the defendants' request for post-judgment taxation of these costs provided they were "reasonable and necessary."[274]

The defendants presented evidence that the search terms and custodians that the plaintiffs asked the defendants to use resulted in a population of more than 400,000 documents.[275] The defendants then employed TAR to narrow the population to a production set of 1,658.[276] The costs defendants sought consisted of payments "to vendors to process documents, conduct coding analytics to identify relevant documents, and to create and maintain a database to store thousands of documents."[277] The court concluded that the defendants' evidence supported the trial court's finding that these costs were reasonable and necessary to the litigation and that the plaintiffs had not shown that finding constituted an abuse of discretion.[278]

In *In re Actos (Pioglitazone) Products Liability Litigation*, in determining common-benefit fees for plaintiffs' counsel in a large MDL, the court awarded attorneys' fees and expenses associated with TAR. It recognized that "[t]his MDL was one of the first to allow the use of a 'predictive coding' system to aid the

273. Dremak v. Urban Outfitters, Inc., No. D071308, 2018 WL 1441834, at *7–8 (Cal. Ct. App. Mar. 23, 2018).

274. *See id*. at *8.

275. *Id*.

276. *Id*.

277. *Id*.

278. *Id*.

discovery process and the production of relevant documents."[279] The court further stated that "the predictive coding system provided a unique way to, in part, realistically manage the immense amount of information needed to be produced and reviewed in this MDL."[280] The court observed that "[t]he predictive coding system, although not perfect or fully realized, nonetheless, provided an innovative efficiency to the discovery process when compared to the existing, prevailing methods of review."[281] The court concluded that the plaintiffs' steering committee and defense counsel "expended tremendous time, and computer and legal expertise, to harness this technological possibility with a quite positive, if not complete, result. As this area involved cutting edge technology, those counsel who could bring their unique expertise and skill to the task were exceptionally valuable to the [plaintiffs' steering committee]."[282]

In *Gabriel Technologies Corp. v. Qualcomm Inc.*, the court awarded more than $2.8 million in fees incurred for the use of "computer assisted, algorithm-driven document review" for almost 12 million documents.[283] The court awarded defendant attorney's fees and TAR-related costs under federal patent law and for misappropriation claims under California's Uniform Trade Secrets Act based on its finding that the plaintiff acted in bad faith by bringing "objectively baseless claims." The court further found that the defendant's use of TAR was "reasonable under the circumstances" of the case.[284]

---

279. *In re* Actos (Pioglitazone) Prods. Liab. Litig., 274 F. Supp. 3d 485, 499 (W.D. La. 2017) (internal citations omitted).

280. *Id*.

281. *Id*.

282. *Id.* at 499–500.

283. Gabriel Techs. Corp. v. Qualcomm Inc., No. 08cv1992 AJB (MDD), 2013 WL 410103, at *10 (S.D. Cal. Feb. 1, 2013).

284. *Id*.

IX. INTERNATIONAL ADOPTION OF TAR

TAR continues to be accepted and discussed in foreign jurisdictions.

The European Court of Human Rights recognized that "courts in at least two jurisdictions (the United Kingdom and Ireland) have approved in recent years the use of technology-assisted review . . . for the purposes of electronic disclosure in high-stakes civil litigation," and reasoned that "[t]he rationale would apply with equal force in criminal cases of comparable complexity."[285] The court further noted that TAR "allows parties to save a significant amount of time and resources in analyzing large data sets."[286]

In Ireland, the Irish High Court in *Irish Bank Resolution Corp. v. Quinn* granted a responding party's motion to use TAR over the objection of the party requesting the production of documents, a ruling upheld by the Irish Court of Appeal.[287]

In England, the English High Court in *David Brown v. BCA Trading* approved the use of TAR over the objection of the requesting party.[288] And in *Pyrrho Investments Ltd. v. MWB Property Ltd.* the parties jointly sought and obtained the approval of the English High Court to use TAR.[289] The same court, in *Astra Asset Management UK Ltd . v. MUSST Investments LLB*, noted

285. Sigurður Einarsson v. Iceland, App. No. 39757/15, Partly Dissenting Opinion of Judge Pavli, (B)(15), Eur. Ct. H.R. Apr. 9, 2019, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-193494%22]}.

286. *Id*.

287. Irish Bank Resol. Corp. v. Quinn, [2015] IEHC 175 (H. Ct.) (Ir.), upheld by the Irish Court of Appeal (*see Court of Appeal Approves use of TAR for Discovery*, MCCANN FITZGERALD (Feb. 25, 2016)).

288. David Brown v. BCA Trading Ltd., [2016] EWHC (Ch) 1464 (Eng.).

289. Pyrrho Inv. Ltd. v. MWB Prop. Ltd., [2016] EWHC (Ch) 256 (Eng.).

that "where a party is intending to use technology assisted review, the intention should be notified to the other party."[290]

A Hong Kong decision also held that a party did not need the court to authorize use of TAR, and "the use of analytic tools of this sort is to be expected" to review large volumes of ESI.[291]

In Canada, in *Perlmutter v. Smith*, the Ontario Superior Court of Justice held that the respondent's counsel could review documents for relevance, not just privilege, where the parties were court-ordered to agree on search terms for the respondent's devices and had also agreed to use TAR.[292] The applicants had unsuccessfully objected to the respondent's counsel "reviewing the documents to narrow the production set generated by TAR other than for privilege."[293] In *PM&C Specialist Contractors Inc. v. Horton CBI Ltd.*, the Alberta Court of Queen's Bench declined to opine on what percentage of document review costs, including TAR, was a recoverable disbursement on a bill of costs.[294]

In *McConnell Dowell v. Santam Ltd*, the Supreme Court of Victoria recognized party agreement on use of TAR and reviewed a TAR report from a Special Referee used to oversee the TAR process.[295] This case is cited in Australia as precedent for use of TAR as an appropriate tool to gain efficiency during the

290. Astra Asset Mgmt. UK Ltd. v. Musst Investments; Musst Holdings Ltd v Astra Asset Mgmt. UK Ltd., [2020] EWHC (Ch) 1871 (Eng.).

291. China Metal Recycling (Holdings) Ltd. (In Liquidation) v. Deloitte Touche Tohmatsu, [2022] H.K.C. 2344 (C.F.I.) (citing, inter alia, Da Silva Moore v. Publicis Groupe, 287 F.R.D. 182, 183 (S.D.N.Y. 2012) and Rio Tinto PLC v. Vale S.A., 306 F.R.D. 125 (S.D.N.Y. 2015)).

292. Perlmutter v. Smith, 2021 ONSC 1372, 2021 CarswellOnt 2055 (2021).

293. *Id*.

294. PM&C Specialist Contractors Inc. v. Horton CBI Ltd., 2017 ABQB 400.

295. McConnell Dowell Constructors (Aust) Pty Ltd. v. Santam Ltd. (No 1) [2016] VSC 734 (Austl.).

eDiscovery process.[296] Furthermore, additional cases have referenced the use of TAR without question to its acceptance.[297] From the decisions, it appears that acceptance of TAR is no longer a threshold issue in Australia, and that when TAR is discussed, it is in general reference to its use or discussion of further details surrounding the process.[298]

296. Mosslmani v. Nationwide News Pty Ltd (No 2), [2018] NSWDC 113 (Austl.).

297. Santos Limited v. Fluor Australia Pty Ltd (No 4), [2021] QSC 296 (Austl.); Viiv Healthcare Co V Gilead Sciences Pty Ltd (No 2), BC202009855; Parbery v QNI Metals Pty Ltd (No. 12), [2018] QSC 276 (Austl.).

298. *See, e.g.,* Viiv Healthcare Co v Gilead Sciences Pty Ltd (No 2), BC202009855 (discussion of TAR interplay with search terms).

X. USE OF TAR IN FEDERAL GOVERNMENT INVESTIGATIONS

Some United States government agencies have accepted the use of TAR for search and review in connection with document productions in regulatory investigations, particularly merger reviews. Implementing TAR in the context of government investigations raises some unsettled questions, and thus the responding party should consider proactively engaging with the government lawyers at the start of the eDiscovery process to discuss what specifications may be acceptable under a TAR protocol (including whether such a protocol is appropriate). Generally, these issues and the specifications for a TAR protocol will be worked out with agency staff on a case-by-case basis at the outset of the production process.

In October 2021, the Federal Trade Commission (FTC) issued an update to its Model Second Request for merger antitrust investigations, which includes specifications related to the use of TAR in response to Second Requests.[299] The Model Second Request expressly contemplates the use of TAR, among other discovery tools, subject to certain requirements. Significantly, the 2021 update requires the responding party to address its intent to use TAR through a written submission to the FTC *prior to* applying TAR to identify responsive documents.[300] This change is meant to more closely align the FTC Second Request process with that of the Department of Justice (DOJ) Antitrust Division.

---

299. Fed. Trade Comm'n, Request for Additional Information and Documentary Material Issued to [Company] (FTC Model Second Request) (revised Oct. 2021), https://www.ftc.gov/system/files/attachments/hsr-resources/model_second_request_-_final_-_october_2021.pdf.

300. *Id.* at 12 (Specification 30), 22 (Instruction I5). *See also* Holly Vedova, *Making the Second Request Process Both More Streamlined and More Rigorous During this Unprecedented Merger Wave*, FED. TRADE COMM'N (Sept. 28, 2021), https://www.ftc.gov/news-events/blogs/competition-matters/2021/09/making-second-request-process-both-more-streamlined.

The responding party also must disclose specified information to the FTC at the end of the document review process.[301] In particular, the responding party must:

> [b](i) describe the collection methodology, including: (a) how the software was utilized to identify responsive documents; (b) the process the Company utilized to identify and validate the seed set documents subject to manual review; (c) the total number of documents reviewed manually; (d) the total number of documents determined non-responsive without manual review; (e) the process the Company used to determine and validate the accuracy of the automatic determinations of responsiveness and non-responsiveness; (f) how the Company handled exceptions ('uncategorized documents'); and (g) if the Company's documents include foreign language documents, whether reviewed manually or by some technology-assisted method; and [b](ii) provide all statistical analyses utilized or generated by the Company or its agents related to the precision, recall, accuracy, validation, or quality of its document production in response to this Request; and [c] identify the Person(s) able to testify on behalf of the Company about information known or reasonably available to the organization, relating to its response to this Specification.[302]

---

301. FTC Model Second Request, at 12 (Specification 30), 22 (Instruction I5).

302. *Id.* at 12 (Specification 30).

The Instructions to the Model Second Request further specify that the responding party must provide to the FTC:[303] "(a) confirmation that subject-matter experts will be reviewing the seed set and training rounds; (b) recall, precision, and confidence-level statistics (or an equivalent); and (c) a validation process that allows Commission representatives to review statistically-significant samples of documents categorized as non-responsive documents by the algorithm."[304]

Similarly, counsel for the Antitrust Division of the Department of Justice has provided guidance regarding TAR protocols in response to Division investigations, updated in March 2021, which also states that the use of TAR should be addressed with the DOJ before embarking on a TAR-based review.[305] Notably, the Instructions section related to Production Format of the DOJ's Model Second Request states the following: "Before using software or technology (including search terms, predictive coding, de-duplication, or similar technologies) to identify or eliminate documents, data, or information potentially responsive to this Request, the Company must submit a written description of the method(s) used to conduct any part of its search."[306] The DOJ Model Second Request also contains the same requirements as the FTC Model Second Request related to confirmation that subject-matter experts will review the seed set and training rounds, disclosure of recall, precision, and confidence-level statistics,

303. Second Request productions tend to use TAR 1.0 procedures, though TAR 2.0 is also in use.

304. FTC Model Second Request, at 22 (Instruction I5).

305. U.S. Dep't of Justice, Request for Additional Information and Documentary Material Issued to [ ] Corporation (DOJ Model Second Request) (revised Mar. 2021), Instructions 3 and 4, https://www.justice.gov/atr/file/706636/download.

306. *Id*.

and a validation process that includes review of statistically significant samples of documents categorized as nonresponsive.[307]

It is important to note that actual practice may deviate from public guidance and policy statements. For example, in 2017, a senior attorney with the Department of Justice, Antitrust Division issued a public statement that the Division would not allow a party to conduct a manual review for responsiveness after the TAR process has been completed.[308] However, the experience of eDiscovery practitioners who regularly engaged with the Division in following years was that the Division did, under certain circumstances, allow some second-level, manual responsiveness review after TAR. Moreover, other Divisions of the Department of Justice routinely allow manual review after the application of TAR. In addition, the DOJ has reserved the right to conduct manual review after TAR in cases where it has represented client agencies as defendants in litigation.

Thus, responding parties should continue to advocate for the most effective use of TAR and negotiate with agency staff to secure a favorable TAR protocol for their clients.

307. *Id*.

308. Tracy Greer, *Avoiding E-Discovery Accidents & Responding to Inevitable Emergencies: A Perspective from the Antitrust Division*, U.S. DEP'T OF JUSTICE (revised Mar. 2017), https://www.justice.gov/atr/page/file/953381/download.

XI. CONCLUSION

Since 2012, case law's broad consensus on TAR has evolved from an acceptable methodology to black letter law that where the responding party reasonably decides to use TAR, courts will permit it. With that acceptance, courts are now grappling with TAR issues involving technical issues, such as search-term culling, recall thresholds, and validation. Courts have been generally consistent in favoring cooperation and transparency among parties on discovery issues, and TAR is no different. While TAR may be an efficient approach for finding relevant documents, courts are not likely to force a TAR process on a reluctant responding party.

TABLE OF CASES

309. This case is also referred to as *Federal Housing Finance Agency v. JP Morgan Chase & Co.*

THE SEDONA CONFERENCE PRIMER ON MANAGING ELECTRONIC DISCOVERY IN SMALL CASES

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

Author:

The Sedona Conference

Drafting Team Leaders:

Greg M. Kohn
Trena M. Patton

Drafting Team:

Hon. Jerome B. Abrams
Kevin M. Clark
Hon. Alice R. Senechal
Gary Soliman
Sean Broderick
Michael J. Scimone
David B. Seserman

Steering Committee Liaisons:

Kimberly J. Duplechain
Greg M. Kohn
Martin T. Tully
Tara S. Emory
Amy Sellars

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 Managing Electronic Discovery in Small Cases,* 24 SEDONA CONF. J. 93 (2023).

PREFACE

Welcome to the final, May 2023 version of *The Sedona Conference Primer on Managing Electronic Discovery in Small Cases ("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.

The intent of this *Primer* is to offer best practices and practical guidance tailored to cases involving smaller quantities or less complex varieties of electronically stored information (ESI) or in which the smaller stakes involved significantly limit the time and money that can and should be spent on electronic discovery. In the interest of the underlying concept of proportionality—tailoring eDiscovery efforts to fit the particular circumstances of the case and resources at hand—some of the guidance provided may diverge from what The Sedona Conference recommends for large, complex cases. But just as in larger cases, cooperation between parties remains central in efficiently managing discovery in small cases and meeting the mandate of Federal Rule of Civil Procedure 1: The just, speedy, and inexpensive determination of every action and proceeding.

This project began with the formation of a brainstorming group in 2018. The passage of time leading to this publication is a reflection of the huge volume and variety of small cases and the difficulty in arriving at common-sense approaches that can be applied uniformly. There is no "one size fits all." The *Primer* was the topic of dialogue at the 2018 Working Group 1 Annual Meeting, the 2019 Midyear and Annual meetings, and, after

considerable reworking, the 2022 Annual Meeting. Previous drafts of the *Primer* were published for member comment in both 2019 and 2022, and for public comment in December 2022. This final version includes revisions based on valuable input provided by Working Group members and the public.

On behalf of The Sedona Conference, I thank drafting team leaders Greg Kohn and Trena Patton for their leadership and commitment to the project. I also recognize and thank drafting team members the Honorable Jerome Abrams, Sean Broderick, Kevin Clark, Michael Scimone, the Honorable Alice Senechal, David Seserman, and Gary Soliman for their dedication and contributions, and Steering Committee liaisons Kimberly J. Duplechain, Tara Emory, Greg Kohn, Amy Sellars, and Martin Tully for their guidance and input. I also thank Stephanie Mitchell and Sonali Ray for their contributions.

We encourage your active participation 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
May 2023

TABLE OF CONTENTS

I. INTRODUCTION

For years, members of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1) have urged the development of a publication on electronic discovery best practices tailored to "small cases"—that is, matters involving little electronically stored information (ESI) and/or where the stakes significantly limit the time and money that realistically can or should be spent on electronic discovery. In response, WG1 has spent what seems to be as many years developing this *Primer on Managing Electronic Discovery in Small Cases (Primer)*. Compared to the effort required to publish papers addressing the challenges of discovery in large, complex litigation, the topic of small cases might seem a minor thing to tackle. It has proved to be anything but.

To begin, most cases are small cases, and most of those are pending in state courts.[1] The sheer volume and variety of small cases make it difficult to offer a singular approach. Unlike larger cases where the financial or public policy stakes are higher, the cost and burden of employing the latest and greatest ESI preservation and production practices may not be necessarily proportional to the needs of a small case or consistent with "the just, speedy, and inexpensive determination of every action and proceeding."[2] Indeed, proportionality is—at bottom—all about tailoring and scaling eDiscovery efforts to fit the particular circumstances, capabilities, and resources at hand. Sometimes, one can only do what one can with the resources available, even if they

1. This *Primer* largely references the Federal Rules of Civil Procedure (Rules 1, 26, 34, etc.), but recognizing that many small cases are litigated in state court, the Primer focuses on general principles that apply across various rules of court and on concepts common in most jurisdictions. Practitioners should consider whether the rules vary in their venues in ways that are significant to the topics discussed.

2. FED. R. CIV. P. 1.

might not be necessarily considered reasonable or defensible in larger matters or different contexts. For this reason, students of other Sedona Conference publications may perceive some of the shortcuts and "MacGyver" solutions discussed in this *Primer* as somewhat at odds with the sage guidance offered in previous papers.[3] Rest assured, The Sedona Conference and the drafting team for this *Primer* continue to heartily endorse those prior papers and best practices and have tried to acknowledge where the suggestions herein may diverge from previous guidance out of practical necessity and based on proportionality considerations. The drafting team merely acknowledges that, in some circumstances, "best practices" themselves might not be proportional to the needs of the case or the means of the parties.

Along with proportionality and the mandate of Federal Rule of Civil Procedure 1, the most important principle in discovery in cases of any size is cooperation, and this *Primer* reinforces and elevates the central role of cooperation in effectively and efficiently managing discovery in small cases.[4] Indeed, "[i]f both requesting and responding parties voluntarily elect to cooperatively evaluate and agree upon the appropriate procedures, methodologies, and technologies to be employed in the case, both may potentially achieve significant monetary savings and non-monetary efficiencies."[5] In short, the parties' informed agreements on the conduct of discovery can become the de facto

3. Merriam-Webster.com defines "MacGyver" as a verb meaning "to make, form, or repair (something) with what is conveniently on hand."

4. The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 125 (2018) [hereinafter *The Sedona Principles, Third Edition*] ("In addition to what is required by those Rules, it is generally in the best interests of the responding party to engage in meaningful cooperation with opposing parties to attempt to reduce the costs and risk associated with the preservation and production of ESI.").

5. *Id*.

best practices as tailored to the matter. Of course, flexibility in electronic preservation and production requires superior communication among the parties. While each party remains in full control of its own destiny,[6] where best practices are departed from out of necessity, efficiency may more likely be achieved through clear communication by the parties about expectations and intentions for discovery processes, including disclosure to[7] and, if feasible, the concurrence of the other party.

As always, however, cooperation may not work in every case, particularly in matters that involve shorter timeframes for negotiating and completing the discovery process. Where the parties cannot reach agreement, thoughtful proportionality arguments will be critical in the event a party must seek judicial support for its proposed electronic discovery approach.[8]

Without doubt, the volume of ESI in the possession of both organizations and individuals increases each year. Cases that would have had little electronic evidence years ago may now require more significant electronic discovery. This *Primer* offers suggestions for managing electronic discovery costs and efforts in proportion to the needs of a small case. In short, the *Primer* embraces a need for bespoke flexibility in small cases that may not be appropriate in other, especially larger, matters. Lest practitioners feel that The Sedona Conference has made "the perfect the enemy of the good," this *Primer* acknowledges the primacy of proportionality, cooperation, and communication as the guiding principles in efficient and cost-effective discovery, particularly when it comes to small cases. The *Primer* also identifies

---

6. *Id*. at 118. ("[T]he case law and the procedural court rules provide that discovery should take place without court intervention, with each party fulfilling its discovery obligations without direction from the court or opposing counsel.").

7. *See* FED. R. CIV. P. 26(a), (f).

8. *The Sedona Principles, Third Edition*, *supra* note 4, at 118.

some low- or no-cost tools and technologies that can help meet small case needs when on a tight budget.

II. WHAT CONSTITUTES A "SMALL CASE"?

This *Primer* is intended to provide guidance to attorneys, parties, and judges in matters that are not large or complex in order to meet the directive of Rule 1 (and its state counterparts) that the Federal Rules of Civil Procedure be "construed, administered, and employed by the court and the parties to secure the just, speedy and inexpensive determination of every action and proceeding." Although the majority of cases implicate ESI, the complexity and expense of electronic discovery can undermine the goals of Rule 1 and the proportionality considerations of Rule 26(b)(1).[9] This may be particularly true in a "small case," regardless of how that term is defined.

Courts have tried to define a "small case" either by the amount in controversy or the type of case. Both of these methods can be helpful to define a small case, but each has shortcomings. Some jurisdictions have implemented rules that limit discovery based upon the relief sought.[10] For example, Utah's Rules of Civil Procedure employ a tiered structure for discovery, based on the amount in controversy identified in the complaint: Tier 1 ($50,000 or less), Tier 2 ($50,001 to $299,999 or non-monetary relief), and Tier 3 ($300,000 and above).[11] The tiers are

9. Under Rule 26(b)(1), the parties are entitled to discovery of matters "relevant to a party's claim or defense and proportional to the needs of the case." The Rule directs that six factors be considered in determining proportionality: "the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." FED. R. CIV. P. 26(b)(1). *See also* The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141 (2017).

10. *See* UTAH R. CIV. P. 26(c)(5), TEX. R. CIV. P. 190.

11. UTAH R. CIV. P. 26(c)(5).

easy to apply, but the approach may undervalue the complexity or the importance of the issues involved in the case. A relatively simple collection matter seeking $300,000 or more would be classified as Tier 3, although there may be little or no electronic discovery necessary; a claim for nonmonetary relief could be considered Tier 2 even though it may implicate public policy and, therefore, require significant electronic discovery. A study of Utah's rule change suggests that practitioners may now be increasing the amount in controversy claimed in the complaint to secure classification at a higher tier with a broader scope of discovery.[12]

The Arizona Rules of Civil Procedure use the case classification method. Arizona also uses a three-tier system, although tiers are not based solely on the relief requested.[13] Instead, the tier to which a case is assigned is "determined by either: (1) stipulation or motion, for good cause shown; (2) placement by the court based on the characteristics of the case; or (3) the sum of the relief sought in the complaint, and any counterclaims or cross-claims."[14]

Under the Arizona method, Tier 1 cases are "simple cases that can be tried in one or two days," such as automobile tort, intentional tort, premises liability, and insurance coverage claims.[15] These are cases with "minimal documentary evidence and few witnesses."[16] These cases will benefit from the strategies in this *Primer*. Under the Arizona rule, a $300,000 collection

12. NATIONAL CENTER FOR STATE COURTS CIVIL JUSTICE INITIATIVE, UTAH: IMPACT OF THE REVISIONS TO RULE 26 ON DISCOVERY PRACTICE IN THE UTAH DISTRICT COURTS 3 (April 2015), *available at* utah-rule-26-evaluation-final-report2015.pdf .

13. ARIZ. R. CIV. P. 26.2.

14. *Id.*, 26.2(c).

15. *Id.*, 26.2(b)(1).

16. *Id*.

case would be classified as Tier 1 because it involves minimal evidence, a few witnesses, and can be tried in one or two days.

Tier 2 cases have "intermediate complexity" and likely involve more than minimal documentary evidence and more than a few witnesses (and may include expert witnesses).[17] Tier 2 cases are likely to involve multiple theories of liability and may involve counterclaims or cross-claims.

Tier 3 cases are logistically or legally complex, such as class actions, antitrust, multiparty commercial or construction cases, securities cases, environmental torts, construction defect cases, medical malpractice cases, product liability cases, and mass torts.[18] These cases may have voluminous documentary evidence, or numerous pretrial motions raising difficult or novel legal issues. Tier 3 cases also require management of a large number of witnesses or separately represented parties or coordination with related actions pending in other courts.[19]

Rather than relying on arbitrary or bright-line rules offered above to define a "small case," the parties should discuss the discovery needs of the case prior to but no later than the Rule 26(f) conference or state court equivalent. The parties should consider all aspects of the case and not focus solely on the amount of monetary relief in controversy or the type of case.[20]

This *Primer* offers the following nonexhaustive list of factors for initial discussion among counsel before the scheduling conference and that should be considered throughout the litigation:

- the proportionality factors, including nonmonetary factors.

17. *Id.*, 26.2(b)(2).
18. *Id.*, 26.2(b)(3).
19. *Id*.
20. *See* FED. R. CIV. P. 26(b).

- the parties' and counsel's familiarity with the facts and issues involved.
- whether the parties and counsel have a reasonable understanding of the scope of necessary discovery.
- whether the parties and counsel have a reasonable understanding of potentially discoverable ESI that might be available.
- whether the documentary evidence is minimal versus "document-intensive."
- whether the subject matter of the case involves a short and discreet time period, since cases involving longer time periods typically involve more potentially discoverable ESI.
- the number of anticipated custodians of ESI and the number of anticipated devices that may contain potentially discoverable ESI.

Consideration of the factors above will help the parties and courts determine the applicability of the strategies in this *Primer*.

III. PROPORTIONALITY CONSIDERATIONS FOR A SMALL CASE

Various aspects of discovery give rise to different burdens, and proportionality considerations may justify creative or simpler approaches for some aspects of discovery within the same case. To understand the burden mitigated by any particular "small case" strategy, it is incumbent upon counsel to understand the difference between such a strategy and ostensible requirements under the discovery rules; be able to quantify that burden, if necessary; and be able to determine that the burden avoided by their client justifies the resulting difference in what is ultimately produced to the requesting party in light of the proportionality factors.[21]

For example, Rule 34(b)(2)(E) requires that ESI be produced in a form requested or, if none is provided, "in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms." This requirement may present a helpful starting point for cooperation in small cases because a form of production that is objectively usable (and likely necessary) in standard cases may not actually be what a requesting party wants to receive in a small case. While a standard ESI production often involves files in a format intended to load into a review platform, a requesting party in a small case may prefer standalone PDFs[22] or native format even if such a production would not contain the information (e.g., metadata) contained in a standard production.

---

21. *See* Sung Gon Kang v. Credit Bureau Connection, Inc., No. 18-CV-01359, 2020 WL 1689708, at *5 (E.D. Cal. Apr. 7, 2020) ("These conclusory, unsupported statements are insufficient to meet Defendant's burden").

22. PDF: Portable Document Format, *The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition*, 21 SEDONA CONF. J. 263, 353 (2020) [hereinafter *The Sedona Conference Glossary, Fifth Edition*].

Counsel in small cases must carefully decide whether adaptations to mitigate costs are justified in light of the needs of the case, including the likely benefit that would be achieved if a more standard approach were taken. Even in small cases, it is possible that the tools and methods employed—particularly for collecting, processing, and producing ESI—may result in problems later in the case or deprive the requesting party of necessary information. In particular, processes that may alter or destroy metadata may affect whether the evidence can be authenticated later and how it can be used.[23]

The court shares the obligation with the parties of ensuring proportional discovery. Where it is available, it is helpful to have the assigned judge guide the parties to the appropriate scope of discovery by implementing case management policies and procedures.[24] The court and counsel should continue to evaluate and adjust the scope of discovery whenever it is reasonable to do so.

23. *See The Sedona Principles, Third Edition*, *supra* note 4, at 169.

24. *See* FED. R. CIV. P. 26(b)(2)(C); *see also* Webinar: Civil Justice Initiative, *It's All About Teamwork: Creating Effective Civil Case Management Teams*, https://www.ncsc.org/Microsites/Civil-Justice-Initiative/Home/Webinars.aspx.

IV. SMALL-CASE TAILORED ELECTRONIC DISCOVERY TIPS

The Sedona Principles, Third Edition[25] contains broad guidance on electronic discovery applicable to civil cases in general. Some aspects of *The Sedona Principles* are particularly salient in small cases. Accordingly, this section focuses on the pragmatic application of those Principles to small cases, including examples of how they might be applied to suit the circumstances of the matter and the resources of the parties.

The focus in small cases is conducting discovery in the most efficient and cost-effective manner. Clients in small cases often are unable or unwilling to budget for expensive processes, a problem that is not unique to electronic discovery. As Sedona Principle 1 makes clear, ESI is generally subject to the same preservation and discovery requirements as other relevant information.[26] What makes ESI different, and at times very burdensome, is its quantity and complexity.

In small cases, discovery is more effective if the parties can simplify the identification and production of relevant ESI and employ strategies to address the volume of ESI as well as the cost of preservation, review, and production. The tips in this *Primer* are geared toward these goals.

A. Early Client Engagement and Process Education

Many parties engaged in small cases may not have experience with litigation or electronic discovery and are often unfamiliar with the process and requirements. This is particularly true when the client is a small organization or an individual. Small organizations may not have a general counsel or information technology (IT) staff; individuals often have no formal organizational "system" for keeping and preserving documents

25. *The Sedona Principles, Third Edition*, *supra* note 4.

26. *Id.*, at 56.

or ESI. Instead, they may simply have devices and systems that they use and interact with as part of their daily routine. In these instances, it is imperative that practitioners educate clients as soon as litigation is reasonably anticipated and throughout the case so that they understand their discovery obligations and can work with counsel to identify and explore options for reasonable and proportional discovery solutions for their small case.

1. Make ESI part of the earliest discussions about the case

At the outset of the case, counsel should inform the client of the obligation to locate and preserve relevant ESI. Counsel should also be sure that the client understands the scope of relevant ESI and the method of preserving ESI in each of the storage locations identified. Many individuals and small organizations may not even be aware of the types and sources of ESI that they possess or have access to, so early communication and discussion on these topics are essential.

2. Conduct custodian interviews

When dealing with an organization, it is important to identify the employees and representatives who have information relevant to the asserted claims and potential defenses. Where possible, speaking with them in real time helps to ensure that sources of discoverable material are properly identified and understood by the client and counsel. When speaking with a custodian about relevant data sources, counsel should ask searching questions to identify where data is located—an essential first step in determining options to access and collect. An excellent and thorough reference point is *The Sedona Conference "Jumpstart Outline."*[27] It may be valuable to spend some time tailoring or

27. Ariana J. Tadler, Kevin F. Brady & Karin Scholz Jenson, *The Sedona Conference "Jumpstart Outline"* (2016), https://thesedonaconference.org/publication/Jumpstart_Outline.

simplifying the questions suggested in the *Jumpstart Outline* to fit the scope of the issues in the case or the client's data sources.

For cases involving several custodians or if circumstances do not permit contemporaneous custodian interviews, counsel may use a standardized written questionnaire for some or all custodians—similar to client interrogatories. At minimum, a conversation at the outset of the case with someone familiar with the relevant data sources can provide counsel with valuable information about relevant ESI and save time and expense at later points in the case.

3. Preservation/Legal Hold

Counsel should educate clients on the need for and methods of reasonably preserving relevant ESI. This should be discussed early to avoid disputes, potential spoliation, and avoidable litigation costs down the road. If the client is an organization, the client should consider the need to send a formal legal-hold notice to employees and non-parties who maintain or possess the client's data and records.[28] Here again, "principles of proportionality should be applied when the costs and burdens of preserving large amounts of ESI may be disproportionate to the needs of the case, and even the sole copy of an ESI item need not be preserved if doing so would be disproportionate to the needs of the case."[29] As such, a party's duty to preserve relevant

28. *See* Alter v. Rocky Point Sch. Dist., No. 13-1100, 2014 WL 4966119, at *8 (E.D.N.Y. Sept. 30, 2014). *See also The Sedona Principles, Third Edition*, *supra* note 4, at 107 ("Parties should also consider whether some preservation notice should be sent to third parties, such as contractors or vendors, including those that provide information technology services.").

29. *Id*. at 94–96.

evidence does not require the freezing of "all documents" and ESI, even if relevant.[30]

Regardless of the form or simplicity of the legal-hold notice, follow-up by counsel is essential to ensure compliance with preservation instructions. Especially in small cases, counsel should never assume that the client has taken steps to preserve relevant ESI. Small organizations and businesses are unlikely to have a formal records retention policy or information governance program, and individuals' organizational systems will vary widely. Instead, counsel should help the client understand how their systems and devices retain and delete data to determine if retention settings need to be adjusted. Examples include changing mailbox size, suspending auto-delete, or enlarging retention periods.

The involvement and direction of counsel is particularly important when the client is an individual. Individuals may rely heavily on devices like smartphones, cloud storage, and laptops that can be lost, broken, or use auto-delete settings. Counsel should consider obtaining backups of clients' devices—including supervising and documenting the process—to avoid any potential spoliation issues that might occur after the preservation obligation is triggered.[31] Many smartphone users automatically back up device data to a cloud service. Clients who do not use cloud backups for their devices should consider doing so during the pendency of litigation (and for data over the relevant time

30. *See, e.g.*, *id.*, at 111, Comment 5.g. ("A party's preservation obligation does not require 'freezing' of all ESI, including all email. Parties need not preserve 'every shred of paper, every e-mail or electronic document, and every backup tape,' nor do they have to go to extraordinary measures to preserve 'all' potentially relevant ESI.") (citing Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003)).

31. *See, e.g.*, Barton & Assocs., Inc. v. Liska, No. 9:19-CV-81023, 2020 WL 8299750, at *2 (S.D. Fla. May 11, 2020).

period), as doing so mitigates the risk of data loss and may lessen the need for more expensive methods of preserving data from mobile devices. At the same time, some clients may need to turn off backups to avoid overwriting an existing backup that may contain unique and relevant information, until the existing backup can be copied.

The aforementioned preservation methods are less thorough than complete forensic imaging, which would also capture logged information like location data that may not be captured by a simple backup. Counsel should engage in a proportionality analysis to determine whether forensic imaging is important to the specific needs of the case. If that analysis shows that forensic imaging (or equivalent preservation method) is not warranted, counsel should consider proactively raising that preservation issue with opposing counsel at the 26(f) conference to avoid later disagreements. It is also important to keep in mind that the cost of eDiscovery services is constantly changing, so counsel should not assume that forensic imaging or other preservation steps are cost prohibitive.

For litigants with older technology and devices, preservation of data on broken/obsolete equipment may be especially important. The client may not have a backup system and may be more likely to use a device to the breaking point rather than upgrade systems that are nearing the end of their usable life.

4. Consider the pros and cons of collection for preservation, as compared with preservation-in-place

In small cases, proportionality must play an important role in determining the reasonable scope of preservation and avoiding the potential costs associated with some forms of collection. In some cases, early collection of ESI may be the appropriate preservation strategy. Collection efforts might include

exporting a key custodian's email account as an Outlook PST[32] file or making a copy of the data on a client's cell phone. Collection for preservation is an important strategy if counsel cannot be sure that the client will undertake appropriate preservation measures, or where the only source of information is a device with some risk of loss or destruction.

When the client is an individual, the collect-to-preserve strategy mitigates the risk that the client is not capable of taking "reasonable" preservation steps as defined in the federal rules and interpreted by the courts. An additional benefit of collecting relevant ESI at the outset of a case is that it may eliminate the need to revisit these data sources with the client for collection later (assuming that new discoverable information will not be created). Early collection may also help counsel prepare for the meet-and-confer process by providing concrete information about the client's data types and volume.

Alternatively, preservation-in-place—i.e., the practice of taking steps to ensure data is preserved where it is stored—may be a more appropriate preservation method, particularly when the likelihood of the ESI being destroyed or lost is low. Factors to consider in weighing the best preservation method include whether the method would impose storage costs (beyond those already allocated by the custodian), whether it would require forensic resources, or whether it would be less convenient than alternatives (for example, where a user's device must be taken into custody). Keep in mind that if discoverable information might be created during the life of the case, collection (or backup) at a single point in time may require counsel to perform additional collection steps later in the case.

---

32. PST: A Microsoft Outlook email storage file containing archived email messages in a compressed format, *The Sedona Conference Glossary, Fifth Edition*, *supra* note 22, at 357.

Cloud-based storage is also important to consider. Most bank accounts, phone accounts, payment histories, and similar services generally offer their users access options that can help identify relevant data, such as filtering and sorting tools. At the same time, these accounts may have deletion schedules, so if these accounts will be important to the case, counsel should ensure that those records are otherwise preserved, which may call for early collection or proactive communication with third-party service providers to ensure the information is not deleted or destroyed.

Some applications owned or used by clients may already contain tools and functionality designed for eDiscovery purposes. For example, enterprise platforms like Microsoft 365 increasingly include eDiscovery tools that may be used to search for content in other platforms or applications. Users can also search mailboxes and sites by using built-in tools to identify, hold, and export content found in such mailboxes and sites.[33] These built-in eDiscovery solutions do have limitations, however, and their capabilities can vary based on licenses, client configurations, and other technical limitations. Counsel should be aware of the capabilities and limitations when using such solutions for preservation, search, and production of ESI in litigation matters of any size.

Text messages from mobile devices are often targets for electronic discovery in litigation and investigations. Failure to preserve and produce relevant mobile device data can result in serious consequences.[34] As discussed in Section V and the *Primer*'s

33. *See* Microsoft Purview eDiscovery Solutions, MICROSOFT, https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide.

34. *See, e.g.*, Paisley Park Enters. v. Boxill, No. 0:17-cv-01212, 2019 WL 1036058 (D. Minn. Mar. 5, 2019) (Court found the defendants acted with "the intent to deprive" in failing to preserve text messages when they failed to

Appendix, several tools might be helpful in inexpensively collecting ESI from mobile devices and generating copies of text message communications.

Beyond email and text messages, new challenges are posed by burgeoning social media and messaging environments, expanded use of ESI stored on collaborative platforms, and other cloud applications and storage. Such environments may require advanced tools and training to manage complex search, collection, and processing efforts.[35] In all cases, counsel will need to identify relevant ESI within these sources as well as cost-effective ways of retrieving or representing it in a reasonably defensible manner. As noted above, it may be cost-effective to investigate the search and export capabilities that already exist within the platform.

5. Consider the pros and cons of properly supervised self-collection vs. other options

Numerous articles and reported decisions have outlined the risks to both clients and attorneys from the self-identification or self-collection of discoverable ESI by custodians, especially if

---

make reasonable efforts to preserve their data and admonished them for their "troubling" and "completely unreasonable" behavior.); Christou v. Beatport, LLC, 849 F. Supp. 2d 1055 (D. Colo. 2012) (Court sanctioned defendant for not taking steps to preserve text messages, which led to a spoliation sanction.).

35. "Costs and risks may increase if the technology makes it more difficult to preserve or collect relevant ESI for litigation. For example, mobile devices that are not synchronized with the organization's servers may require physical collection of the mobile device to meet preservation or discovery obligations if there is unique, relevant ESI on the device that the IT or legal group cannot collect from the organization's servers." *The Sedona Principles, Third Edition*, *supra* note 4, at 63.

they are interested parties.[36] The case law is clear that self-collection of ESI by a client raises a real risk that data could be destroyed (including metadata in the collection process), altered, or otherwise corrupted. Indeed, there are many dangers inherent in self-collection, including good-faith omission by inadvertence, insufficient diligence, or lack of technical or legal training.[37] To be sure, a custodian or its IT professional may not possess the knowledge of how to collect data in a manner that avoids spoliation of file contents and its metadata. Further, as discussed in Section III.F.2, self-collection of ESI may not be self-authenticating because custodians or in-house IT staff might not possess the tools necessary to produce the authenticating hash values necessary to meet the "authenticated . . . process of digital identification" for self-authentication under Federal Rule of Evidence 902(14).[38]

Importantly, though, the disdain for self-collection most commonly expressed by courts and commentators stems from counsel's complete delegation and failure to properly supervise the client's search and retrieval of discoverable ESI.[39] In this

---

36. *See, e.g.*, Equal Emp't Opportunity Comm'n v. M1 5100 Corp., No. 19-cv-81320, 2020 WL 3581372 (S.D. Fla. July 2, 2020) (Explaining reasons why attorneys should not allow clients to self-collect potentially relevant ESI.); Nat'l Day Laborer Org. Network v. U.S. Immigration and Customs Enf't Agency, 877 F. Supp. 2d 87 (S.D.N.Y. 2012) ("Searching for an answer on Google (or Westlaw or Lexis) is very different from searching for *all* responsive documents in the FOIA or e-discovery context . . . " and "most custodians cannot be 'trusted'" to effectuate a legally sufficient collection.).

37. *See, e.g.* Green v. Blitz U.S.A., Inc., 2011 WL 806011, 2:07-CV-372 (TJW), at *6, n.5 (E.D. Tex. Mar. 1, 2011) ("That Blitz put someone in charge of its discovery who knows nothing about computers does not help Blitz's effort to show that it was reasonable in its discovery obligations.").

38. FED. R. EVID. 902(14).

39. "Self-collections by custodians may give rise to questions regarding the accuracy and completeness of collections if directions and oversight by

regard, "[t]he relevant rules and case law establish that an attorney has a duty and obligation to have knowledge of, supervise, or counsel the client's discovery search, collection, and production."[40] There are circumstances under which custodian self-collection—diligently supervised by counsel or a service provider acting at counsel's direction—may satisfy counsel's certification obligations under Rule 26(g)(1). Because collecting data must be done carefully, and all aspects must be completely and accurately documented, counsel should consider investing in training on how to supervise and/or implement defensible collection procedures.

While self-identification and collection of potentially responsive documents by custodians is not usually recommended, as noted above, there are scenarios in which it may be proportional and defensible, so long as a reasonable process is followed and documented. This process includes providing a timely and detailed legal-hold notice and providing instruction to custodians on how to identify potentially relevant documents and perform the self-collection, including how and where to store or transfer the collected information. The process should be documented, and counsel should make themselves available

---

legal counsel or forensics experts are poor or non-existent." *The Sedona Principles, Third Edition*, *supra* note 4, at 168.

40. *Equal Emp't Opportunity Comm'n*, 2020 WL 3581372, at *2 ("It is clear to the Court that an attorney cannot abandon his professional and ethical duties imposed by the applicable rules and case law and permit an interested party or person to "self-collect" discovery without any attorney advice, supervision, or knowledge of the process utilized.").

to answer questions that custodians may have throughout the process.[41][42]

Counsel in a small case may determine that self-collection poses undue risk *and* that preservation through a full forensic collection performed by an outside eDiscovery vendor is disproportionately costly, burdensome, and disruptive to operations given the needs of the case.[43] Accordingly, counsel may justifiably adopt an approach that, while not consistent with "best practices," may still produce a forensically sound copy of the data[44] by using tools, trained individuals, and proper documentation of the steps taken.

---

41. *See* Mirmina v. Genpact LLC, 2017 WL 3189027, Civil No. 3:16CV00614(AWT) (D. Conn. July 27, 2017) (Where defendant's in-house counsel supervised and documented the preservation and search process, the court denied plaintiff's motion to compel additional responsive electronic communications despite the fact that an individual directly involved in the underlying claims of the suit "self-identified" potentially responsive emails.).

42. To ensure that self-collection actually saves costs, counsel should look for ways to make the process streamlined and repeatable, such as having simple, easy-to-follow instructions or tutorials on how to export from common sources like Gmail or Outlook. These instructions may need to be updated periodically to reflect technical changes and/or upgrades.

43. "Forensic data collection requires intrusive access to desktop, server, laptop, or other hard drives or media storage devices . . . . However, making a forensic copy of computers is only the first step of an expensive, complex, and difficult process of data analysis that can divert litigation into side issues and satellite disputes involving the interpretation of potentially ambiguous forensic evidence." *The Sedona Principles, Third Edition*, *supra* note 4, at 140–41.

44. *See The Sedona Conference Glossary: Fifth Edition*, *supra* note 22, at 312 (defining "Forensic Copy").

B. Preliminary Considerations and the Rule 26(f) conference

1. Dialogue at the beginning of the case

Early case management conferences, such as the Rule 26(f) conference under the Federal Rules, are an often-missed opportunity to address ESI issues that are specific to small cases. Reference guides, such as *The Sedona Conference "Jumpstart Outline,"*[45] may be beneficial to tee up key questions to frame the scope of electronic discovery. Engaging in dialogue regarding eDiscovery and anticipating issues will help avoid costly disputes, especially when counsel wants to select low-cost eDiscovery solutions that may have shortcomings but may be proportional for the small case. Be prepared to educate opposing counsel, if necessary, to facilitate a productive discussion. Mutual education and cooperation can save time and money in small cases by addressing eDiscovery early. In jurisdictions that do not require early disclosure, or if such disclosures are honored more in the breach than the observance, requesting parties may consider using early discovery devices such as a small number of focused interrogatories to achieve the same goal. Identifying a custodian or the name of a database this way may save weeks or months of meet-and-confer time.

2. Don't be coy

Requesting parties should avoid the temptation to play it close to the vest by not disclosing the kinds of ESI they will seek. When litigating in venues that permit early delivery of discovery requests (see, e.g., Rule 26(d)(2)), consider delivering Rule 34 requests before the case management conference to frame the discussion of the nature and sources of responsive documents.

---

45. Tadler et al., *supra* note 27.

Neither party is required to limit its disclosures to the information called for by Rule 26 or local guidelines. For example, counsel may consider disclosing the discovery platform it will use (if any) to review and categorize documents.[46] This can lead to multiple opportunities to save costs, if the party receiving that information is familiar with the platform. Although there is wide variation, many review platforms have analytics and other features included for no additional charge, or at modest cost, but those platforms will require that the data loaded into them is formatted a certain way. If a requesting party wants to use a platform and the other party is unfamiliar with it, the parties should confer to resolve any issues with form of production and the extent to which searchable text and/or metadata will be produced.[47]

3. Strive to reach agreement

Sedona Principle 3 stresses the importance of reaching an agreement on discovery issues early and cooperatively.[48] This is especially important in small cases where clients have limited resources. Cooperation can lead to significant cost savings for all parties. Early, informal discussions between counsel about dates at issue, potential search terms and custodians, and data collection methods can move the case forward quickly and avoid motion practice. Some time- and cost-saving agreement points may include:

- the date range of discoverable ESI;

---

46. *See In re* Valsartan, Losartan & Irbesartan Prods. Liab. Litig., No. 19-2875, 2020 WL 7054284 (D.N.J. Dec. 2, 2020) (requiring parties to meet and confer regarding ESI discovery).

47. *See infra* Appendix for examples of discovery platforms currently available on the market.

48. *The Sedona Principles, Third Edition*, *supra* note 4; *see also* The Sedona Conference, *Cooperation Proclamation*, 10 SEDONA CONF. J. 331 (2009 Supp.).

- custodians and noncustodial sources of ESI;
- search terms or other methods of searching data, such as email domains;
- methods for searching databases containing relevant information, such as the filters or fields that can be readily searched;
- an exchange of "hit counts" that help identify overinclusive search terms to avoid burden arguments; and
- a sampling exercise in which small batches of ESI that hit on key terms or other criteria are reviewed to see if the documents are relevant.

Suggesting and then reaching agreement on alternative and simpler ways to capture and produce relevant information can sometimes go a long way. For example, an individual faced with responding to a government subpoena or civil investigative demand may not have the resources to engage a vendor to conduct a forensic collection of text messages from the user's cell phone. By promptly raising the issue with the requesting agency, it may be possible to reach agreement that the individual be permitted to instead produce screenshots of the responsive text messages—so long as the underlying native data is separately preserved in place and intact (i.e., via a backup).

4. Focus on accessibility

Sedona Principle 8 is particularly applicable here.[49] Especially in a small case, first focus on the ESI that is easiest to

49. "The primary sources of electronically stored information to be preserved and produced should be those readily accessible in the ordinary course. Only when electronically stored information is not available through such primary sources should parties move down a continuum of less accessible sources until the information requested to be preserved or produced is

collect, produce, and review, which in many instances may be more than enough to achieve a resolution of the dispute. Start with what the parties agree on, such as the most relevant custodians, the most accessible data sources, or agreed-upon searches. Use this data to evaluate whether the agreed search parameters are effective. Leave open the possibility that search terms and other limitations may be modified and narrowed as parties become more familiar with the data.

Counsel may do well to prioritize the most important information, since processing, review, and production costs are directly proportional to the volume of ESI. This approach may support a proportionality analysis against needing to collect data from more difficult or expensive sources that are less accessible for technical or other reasons.[50]

5. Address "Bring Your Own Device" issues

Some organizations allow employees to use personal devices for business purposes, often under a "Bring Your Own Device" (BYOD) policy or agreement. The use of personal devices and accounts at work may mean that business information responsive to litigation is commingled with an employee's personal information. The reverse may also be true—an employee may have stored personal information on a device owned by the organization. These situations trigger privacy concerns and

---

no longer proportional." *The Sedona Principles, Third Edition*, *supra* note 4, at 134.

50. The Sedona Conference, *Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible*, 10 SEDONA CONF. J. 281 (2009), *available at* https://thesedonaconference.org/publication/Commentary_on_Preservation_Management_and_Identification_of_Sources_of_Information_that_are_Not_Reasonably_Accessible.

rights under local or state law.[51] A company may not be able to compel an employee to turn over a personal device for inspection or collection, even when a BYOD policy or agreement is in place.[52]

Such issues often arise as a question of whether the responding party has possession, custody, or control of the personal device. While a full discussion of these issues is jurisdiction specific and beyond the scope of this *Primer*,[53] it will be helpful to identify whether there are BYOD sources at issue and what position the responding party will take regarding its control over information stored on those devices.

Before insisting on the collection of data from these devices, consider the following questions:

- Is the data on the device unique, or is it a copy of data that can more easily be collected from laptops, computers, or applications in the possession, custody, or control of the producing party?
- Is the data on the device critical to the claims and defenses in the case, or is data from other sources sufficient?
- Does the responding party have a BYOD policy or agreement, and what are the terms of that policy?

---

51. *See* The Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 SEDONA CONF. J. 495 (2018).

52. *See, e.g.*, Hayse v. City of Melvindale, No. 17-13294, 2018 WL 3655138, (E.D. Mich. Aug 2, 2018).

53. *See* The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* 17 SEDONA CONF. J. 467, 527 (2016) for a more detailed discussion of the topic. The *Commentary* addresses the variation in approaches taken by different jurisdictions.

- Does the responding party have the legal right to obtain relevant information stored on its employees' devices?
- Does the responding party have the practical ability to obtain relevant information stored on its employees' devices?[54]

Regardless of who controls a BYOD device, preservation of these devices early on, as set forth above, is important. Even if the responding party is not in control of the devices, it may still need to notify the device owner for preservation purposes. The Appendix to this *Primer* includes a nonexhaustive, representative sample of some of the least costly and technically simple applications and technologies to collect and preserve ESI from mobile devices.

6. ESI Protocols

In some large or complex matters, the parties may find it desirable to establish an ESI protocol early in the case to document agreement as to the scope of preservation, the procedures to search for responsive documents, and form of production. Negotiations and protocols addressing discovery of ESI help set expectations for each party about the other's needs and plans, particularly on the issue of production format. For example, production in searchable PDF or native formats may be preferred in small cases. However, if the production includes hundreds or thousands of emails, production in PDF format may not be appropriate due to the loss of searchability and metadata. For some file types, such as spreadsheets and presentations,

54. Note that the previous two questions will be appropriate in different jurisdictions based on how that jurisdiction interprets "control." *See Id.* at 482–91. Whether or not the responding party is required to notify the requesting party that the information sought is in the hands of a third party is also jurisdiction specific. *Id.* at 483.

native files may be preferred because they are difficult to review once converted to images or static form.

However, the process of negotiating, drafting, and complying with an ESI protocol may be too impractical, time consuming, or costly in a small case. Regardless, counsel should document their agreement to the form of production even if a formal or more extensive ESI protocol is not warranted. Such an agreement can prevent later confusion and arguments over document production.[55] If agreement is not possible or preferred, the responding party may wish to clearly disclose its intended form of production if it is not what was requested.

If the production includes data types with which either party's counsel may be less familiar, such as text messages or communications from channels such as Teams, Slack, or WhatsApp, consider including a protocol for the production of these data types *only* if counsel fully understands the complexities and costs of collecting, searching, and producing such ESI. In the absence of a protocol, counsel should consult the default requirements of Rule 34(b)(2)(E)(i)-(ii) or the local rule for the form of production and address other topics through the meet-and-confer process as they arise.

C. Discovery Requests & Responses

1. Avoid boilerplate requests and responses

Sedona Principle 4 has long recognized the importance of specificity in both document requests and responses.[56] Subsequent Sedona publications have similarly urged litigants to

---

55. *See* Corker v. Costco Wholesale, No. C19-0290RSL, 2020 WL 1987060 (W.D. Wash. Apr. 27, 2020); Lundine v. Gates Corp., No. 18-1235-EFM, 2020 WL 1503514 (D. Kan. Mar. 30, 2020).

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

avoid vague responses and boilerplate objections to document requests, providing guidance on how to effectively do so.[57] Yet, despite the changes made to Rule 34 in December 2015 regarding specificity, parties frequently fail to follow the requirements of the Rule.[58]

Boilerplate requests or responses tend to be counterproductive because they lead to ambiguity and additional time spent meeting and conferring before the parties settle down to the actual information being sought or produced. This can be especially problematic in a small case, particularly when discovery periods are short. A request for all documents on a very broad topic (especially one couched in language like, ". . . that refer or relate to . . .") is even less likely to net additional documents in a small case if the universe of documents is relatively small.

Responses will be most effective in limiting cost when they disclose the scope and limits of the search or production that a responding party undertakes. For example, a party may agree to search a shared drive or the workstation of a single custodian but object on burden/proportionality grounds to searching mobile devices or social media. Disclosure informs the meet-and-confer process and can facilitate compromise on the scope of discovery.

---

57. *See* 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).

58. *See, e.g.*, Mancia v. Mayflower Textile Servs. Co., 253 F.R.D. 354, 358 (D. Md. 2008); Fischer v. Forrest, 14 Civ. 1304 (PAE) (AJP), 14 Civ. 1307 (PAE) (AJP), 2017 WL 773694, (S.D.N.Y. Feb. 28, 2017); CBF Industria de Gusa S/A v. AMCI Holdings, Inc., 13-CV-2581, 2019 WL 3334503 (S.D.N.Y. July 25, 2019).

2. Don't wait to produce

Though the rules allow responding parties to file responses before producing documents,[59] in a small case it may be more efficient to produce documents with the discovery responses. This allows the requesting party to evaluate the documents produced and assess whether the production is sufficient. Objections are often drafted before the responding party's counsel reviews the document production, but conferring about those objections before reviewing the documents may lead to pointless disputes.

3. Be practical about making and logging claims of privilege

"Logging large volumes of withheld ESI is often costly, burdensome, time-consuming, and disproportionate to the needs of the case."[60] The Federal Rules of Civil Procedure (and the state rules that follow them) do not explicitly require privilege logs.[61] If the parties can openly discuss what the privilege issues are and how they might be resolved, then the parties might agree that they may not need to exchange privilege logs.[62] This may

59. FED. R. CIV. P. 34(b).

60. *The Sedona Principles, Third Edition*, *supra* note 4, at 159 (internal citations omitted). "In addition, logging ESI such as email strings and attachments is difficult and lacks any uniform standard. Reviewing, redacting, and logging metadata or embedded information similarly can be a significant and undue burden." *Id.*

61. FED. R. CIV. P. 26(b)(5)(A) (requiring that the party making a claim of privilege disclose sufficient information for the other parties to assess the claim).

62. *Contra* Desoto Health & Rehab, L.L.C. v. Philadelphia Indem. Ins. Co., No. 2:09-CV-599-FTM-99S, 2010 WL 4853891, at *2 (M.D. Fla. Nov. 22, 2010) ("Agreements [not to produce privilege logs] are not controlling on this Court as the requirement to file privilege logs is not only for the parties, but also for the Court to use in evaluating the sufficiency of a privilege claim.

be especially true in a small case, where large volumes of ESI are less likely and where counsel is less likely to have been involved in pre-litigation communications. If a privilege log is needed, the parties should discuss how logging effort can be done to keep costs low.

Federal Rule of Evidence 502(d) provides heightened protection against waiver in instances where privileged information is knowingly or unknowingly disclosed. A 502(d) order or equivalent is useful for all parties in cases of all sizes, and The Sedona Conference recommends the entry of 502(d) orders as a best practice.[63]

D. Use Technology to Achieve Cost Savings

1. Use (all available) technology to your advantage

Although ESI has vastly expanded the universe of documents that are relevant to any dispute, technology provides ways to manage that volume. Even the relatively simple technology of keyword searching was little known 20 years ago. Since then, technologies that are far more sophisticated have emerged.[64] Section VI of this *Primer* discusses further the use of

---

Therefore, the Plaintiff is still required, by this Court, to complete privilege logs . . . ."); *see also* Williams v. Taser Int'l, Inc., 274 F.R.D. 694, 696 (N.D. Ga. 2008) (requiring log for all claims of privilege); S.C. Coastal Conservation League v. Ross, 431 F. Supp. 3d 719, 725 (D.S.C. 2020) (requiring an index to determine whether documents were improperly excluded from production).

63. *See* The Sedona Conference, *Commentary on the Effective Use of Federal Rule of Evidence 502(d) Orders*, 23 SEDONA CONF. J. 1 (2022); *See also* The Sedona Conference, *Commentary on Protection of Privileged ESI*, 17 SEDONA CONF. J. 95 (2016).

64. The Sedona Conference, *Best Practices Commentary on the Use of Search & Information Retrieval Methods in E-Discovery*, 15 SEDONA CONF. J. 217 (2014); The Sedona Conference, *TAR Case Law Primer*, 18 SEDONA CONF. J. 1 (2017).

such technologies in small cases. Sedona Principle 11,[65] which recommends the use of technology to achieve cost savings, also has particular application to small cases. When considering technologies in the meet-and-confer process, counsel should consider the technologies available to all parties. Particularly in asymmetrical litigation, a party with greater resources at its disposal may be better positioned to deploy technology, even in a small case where it might not otherwise be available.

2. Combine technology with good process

Consideration should be given in small cases to how best to design the collection and search process to save costs and limit volume. Tools are only as effective as the skill of the user. Cost-effective and defensible use of tools requires intelligent processes and workflows.[66] For example, it can be more efficient to target a search against a selected universe of documents from the sources most likely to have relevant data, rather than applying search technologies to a broader universe of ESI that includes sources unlikely to contain relevant data or that contain data that does not lend itself to the search methodology. Counsel should understand the different types of searching available and whether searches will be effective given the tools they intend to use and the form of the data received. For example, some searches may be fielded, meaning they can be run against specific categories of information contained in file metadata (e.g., the subject line of an email, date, To/From, etc.). However, such searches require the fields to be intact when counsel handles

65. *The Sedona Principles, Third Edition*, *supra* note 4, at 164 ("A responding party may satisfy its good faith obligations to preserve and produce relevant electronically stored information by using technology and processes, such as sampling, searching, or the use of selection criteria.").

66. The Sedona Conference, *Commentary on Achieving Quality in the E-Discovery Process*, 15 SEDONA CONF. J. 265 (2014).

them, and an application that allows searching the specific fields.

E. Discovery Motion Practice

Discovery motions are a frequent—and costly—element of pretrial practice and litigation. Courts encourage parties to resolve such disputes informally through mandatory meet-and-confer requirements. When motion practice is necessary, parties should continue to look for ways to reduce the cost and complexity of ESI-related motions.

1. Consider agreeing to streamlined motion procedures, if allowed

Courts differ in how they ask parties to present discovery motions. Because ESI can often be time-sensitive, consider agreeing in advance to use expedited motion procedures. These may include letter briefs, joint presentation of issues in a single filing, or shortened timetables for filing the motion and response. Where allowed, these procedures can save time and cost.

2. Avoid the jargon

Electronic discovery can be daunting because of the wealth of technical information and specialized terminology. Advocates should aim to cut through these obstacles to make issues clear and accessible for clients, opposing counsel, and the court.

3. Pick your battles

Strategic prioritization of high-impact issues is always good advice, but be mindful that electronic discovery can be costly. Especially in a small case, the cost of discovery may outweigh the value of the case. The parties' ability to cooperate, reach agreement, and limit issues in dispute will avoid motion fights.

When a discovery motion is filed, showing the court that an honest effort was made to resolve the dispute informally may convince the court that counsel's discovery demands are reasonable.

F. Deploying ESI as Evidence in Small Cases

As with all evidence, ESI must ordinarily meet the requirements of admissibility and authentication. Modern courtroom technology is generally geared toward the use of ESI, so know ahead of time how to use it to present the case.

1. Plan for authentication and presentation

Until recently, the Federal Rules of Evidence governing admissibility did not separately address the admissibility of ESI.[67] The primary difference between ESI and other evidence is the process of authentication.[68] In some ways, ESI makes it easier for parties to stipulate to authenticity—e.g., it is likely that an email produced from a server is an authentic representation of the original document. [69] On the other hand, ESI can also present unique authentication challenges, and the parties and courts should discuss whether the parties should stipulate to the authenticity of all or some ESI produced, depending on the data source, form of production, and/or availability of metadata or other indicia of authenticity.[70] To keep costs low, parties should

67. FED. R. EVID. 901-903.

68. FED. R. EVID. 902(13)-(14).

69. *See* U.S. v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006) (finding email communications authentic under Federal Rule of Evidence 901 on the basis of characteristics such as domain).

70. *See* FED. R. CIV. P. 36 (permitting a party to request admission of the "genuineness of documents" from an opponent); FED. R. CIV. P. 16(C)(3) (allowing parties to request that an opposing party stipulate "regarding the authenticity of documents"; FED. R. CIV. P. 26(a)(3) (requiring that parties raise

stipulate to authenticity when reasonable. Such stipulations, of course, depend on the proportionality factors and should be delayed until *after* the ESI has been produced.[71]

Because ESI is used in different ways at different points throughout a case, different forms of production may be better or worse suited than others. For example, some technologies for producing text messages can export the relevant communications to an Excel file. This may make them easier to review, especially at large volumes, but the resulting report does not look at all like the text message that the user actually sent or received. So, when introducing the message as an exhibit, the witness may be less likely to recognize it. At trial, too, an entry in an Excel file may have far less visual impact than a text message that is in a form most jurors are familiar with.

On the other hand, some files are less likely to be presented at trial but will be important to other needs in the case and thus require different forms of production. For example, data compilations that will need to be sorted or analyzed by an expert are often best produced in an Excel or .csv file.[72]

Take these needs into account when negotiating forms of production. If documents are less likely to be used as exhibits at trial, as in the data example above, then authentication by certificate is likely sufficient. If a given document is important for visual impact, as in the case of text messages, be sure to seek it

---

within 14 days any objections to the authenticity of documents and exhibits in pretrial disclosures).

71. *See, e.g.*, Rossbach v. Montefiore Med. Ctr., 19cv5758 (DLC), 2021 WL 3421569 (S.D.N.Y. Aug. 5, 2021) (dismissing plaintiff's wrongful termination claims after finding plaintiff perpetrated a fraud on the court by introducing as evidence a fabricated text message).

72. CSV: Comma Separated Value, *The Sedona Conference Glossary, Fifth Edition*, *supra* note 22, at 281.

in a form that will meet those needs and can be easily authenticated by the relevant witness.

2. Know and use the authentication rules

In instances where a stipulation is not possible, authenticating ESI has become more efficient and cost-effective. On December 1, 2017, Federal Rule of Evidence 902 was updated to allow parties to authenticate certain electronic evidence by methods other than the testimony of a foundation witness.[73] The updated rule provides that electronic data recovered "by a process of digital identification" is self-authenticating and does not require the trial testimony of a forensic or technical expert where best practices are employed, as certified through a written affidavit by a "qualified person" who utilizes best practices for the collection, preservation, and verification of the digital evidence sought to be admitted.[74] This can help reduce costs by avoiding expensive and burdensome in-person trial testimony.[75] Because the amended Rule 902 requires that ESI contain information needed for "digital identification," counsel should consider such requirements early on, especially when undertaking any proportionality analysis that could later affect authentication.

3. Consider the costs for ESI presentation at trial

In a small case, counsel likely will need to operate trial technology themselves. The good news is that there is a wide range of software available for this purpose, at relatively low cost, and much of it is very user-friendly. One caveat is to ensure that the ESI being presented is in a form that the presentation software

73. FED. R. EVID. 902(13)-(14).

74. The Sedona Conference, *Commentary on ESI Evidence & Admissibility, Second Edition*, 22 SEDONA CONF. J. 83 (2021).

75. FED. R. EVID. 902(13)-(14) advisory committee's notes to 2017 amendment.

can use—e.g., if an application uses only PDFs, an Excel file may call for a different solution.

4. Consider the form of presentation when determining the form of production

ESI can be presented in the traditional static form (PDF or TIFF[76] images), hard copy, near-native, or in native form—the form in which the ESI was created and maintained. So long as it is proportional to do so, counsel should request ESI in the form in which it will be most usable for case preparation and presentation.[77] For example, a PowerPoint presentation that includes dynamic slides may be more effective when presented at trial in its native form. In contrast, a static image of a text message sent via smartphone may be more useful for counsel to present at trial, as it will look more "familiar" than an extracted SMS message.

76. TIFF: Tagged Image File Format: A widely used and supported graphic file format for storing bit-mapped images, with many different compression formats and resolutions, *The Sedona Conference Glossary, Fifth Edition*, *supra* note 22, at 377.

77. *See* Sedona Principle 12. Moreover, "[p]arties should not demand forms of production, including native files and metadata fields, for which they have no practical use or that do not materially aid in the discovery process." *The Sedona Principles, Third Edition*, *supra* note 4, at 173.

V. MANAGING SMALL-CASE DISCOVERY FROM THE BENCH

Judicial management is critical to efficient discovery in small cases. Different courts have different philosophies concerning the management responsibilities of the judge. Some courts have rules-driven approaches concerning when and how small cases proceed.[78] Upon filing, discovery rules are triggered either by case type or value.[79] Some courts rely on judges or nonjudicial case managers to conduct some type of triage and issue directives incorporating the discovery plan. In general, small-case discovery is largely a product of local rules and legal culture, and the court sets expectations for practitioners. Regardless of the source of direction for discovery, it is incumbent on the court to provide early guidance.

Electronic discovery presents an opportunity for judges to engage with counsel to promote efficiency and keep costs down. ESI and the technology associated with it is ever-changing. Judges may consider asking counsel questions about the ESI at issue in the case. Courts should be open to information and education about ESI from the parties and should feel free to request letter briefs or additional information about the parties' data, systems, and potential ESI challenges. Practitioners should be prepared to bring the court's ESI questions to their clients for further information and explanation.

---

78. CIVIL JUSTICE COMMITTEE, CALL TO ACTION: ACHIEVING CIVIL JUSTICE FOR ALL, APPENDIX D: PILOT PROJECTS, RULE CHANGES, AND OTHER INNOVATIONS IN STATE COURTS AROUND THE COUNTRY (2016), *available at* https://www.ncsc.org/__data/assets/pdf_file/0022/25681/ncsc-cji-appendices-d.pdf.

79. Commercial Court, Maricopa County, Experimental Rule 8.1 (2017), https://superiorcourt.maricopa.gov/media/1098/rule-81.pdf; Minnesota Special Rules For The Pilot Expedited Civil Litigation Track 1-4 (2017), https://www.mncourts.gov/Documents/0/Public/Rules/Special_Rules_for_Pilot_ELT.pdf; UTAH R. SMALL CLAIMS P. (2018), https://legacy.utcourts.gov/rules/srpe.php.

1. Mandatory disclosures

Initial mandatory disclosures are critical to determining whether a case is "small." Courts should require disclosures sufficient to determine whether small-case rules and procedures are appropriate, either through general jurisdiction practice rules or individual case management rules.

2. Query parties about data needs, technology tools, and plans

Judges should be sure that the parties have discussed the form of production and the use of technology for production. Information from this discussion may inform the likely scope of discovery and production format.[80] Judges should question counsel about the technology resources at their disposal. If firms or clients have already invested in discovery tools, the capabilities of the tools may inform appropriate discovery processes for the case. A discussion of file types is key for a potential native production, especially when the files originate from proprietary applications, and native file production may result in a loss of metadata without the correct tools and collection process.

3. Apply common-sense preservation obligations

Judges may want to encourage counsel to confirm that clients understand preservation obligations and how to take steps to preserve data. Preservation of ESI in small cases should be understood to include metadata for disclosed documents. For example, while data from mobile devices and USB drives may not be required for initial disclosures, counsel should be sure that clients understand that preservation requirements might mean they cannot upgrade devices, change retention on devices, or clean off storage drives during the pendency of the

80. *See* ESI Protocols, *supra* Sec. IV.B.6, discussing production format.

litigation, or that they must take affirmative steps to prevent the deletion of ESI, such as changing retention settings on applications or mobile devices.

4. Provide orders to set parties' expectations regarding timelines

The first key order in a small case is the Scheduling Order, which should direct the timing of all events, including mandatory disclosures (if applicable), motion practice (e.g., discovery and dispositive motions), exhibit and witness lists, and objections. While this may be the norm in federal court cases, it may not be likely in state court cases. The timing and deadlines should be scaled in a manner consistent with jurisdictional disposition expectations.

5. Expedite resolution of discovery disputes

In small cases, it is helpful for the judge to provide expedited discovery dispute resolution.[81] This allows the parties to quickly and cost-effectively get a decision on discovery disputes in a manner that does not require a formal motion. The meet-and-confer process is important but is not a panacea. Judges may want to encourage the parties to engage with the court during the meet-and-confer process before the issue escalates to motion practice. The court can be helpful in establishing the goals, benchmarks, and timetables (see Section III.B.1.c) that will move the parties toward a stipulation that avoids later disputes and facilitates the resolution of the case.[82]

---

81. There are many examples (*see* MINN. GEN. R. PRAC. 115.04 (d) (2019); S.D.N.Y. R. 37.2 (2018).

82. Additional Materials:

- FEDERAL JUDICIAL CENTER, PILOT PROJECT REGARDING INITIAL DISCOVERY PROTOCOLS FOR EMPLOYMENT CASES ALLEGING ADVERSE ACTION (2011), *available at* https://iaals.du.edu/sites/

default/files/documents/publications/federal_employment_protocols_pilot_project.pdf.

- RONALD J. HEDGES, BARBARA JACOBS ROTHSTEIN & ELIZABETH C. WIGGINS, MANAGING DISCOVERY OF ELECTRONIC INFORMATION, THIRD EDITION (2017), FEDERAL JUDICIARY CENTER, *available at* https://www.fjc.gov/sites/default/files/materials/38/Managing%20Discovery%20of%20Electronic%20Information_Third%20Edition_Second%20Printing_2019.pdf.
- TIMOTHY T. TAU & EMERY G. LEE III, TECHNOLOGY-ASSISTED REVIEW FOR DISCOVERY REQUESTS: A POCKET GUIDE FOR JUDGES (2017), FEDERAL JUDICIAL CENTER, *available at* https://www.fjc.gov/sites/default/files/2017/Technology-Assisted%20Review%20for%20Discovery%20Requests.pdf.
- *Commentary on ESI Evidence and Admissibility, Second Edition*, *supra* note 74.

VI. COST-EFFECTIVE USE OF DISCOVERY TECHNOLOGY IN SMALL CASES

As discussed above, the types and volumes of ESI are ever expanding. Even in small cases, electronic discovery may implicate significant amounts of ESI, of which only a small fraction may be relevant. For example, an employment matter may require an email collection spanning the employee's tenure and multiple custodians, capturing ESI unrelated to the claims and defenses in the case. A personal injury or medical malpractice matter may require the production of photos, text messages, and social media. Each year, new technology is developed to improve electronic discovery efficiency and reduce overall litigation costs. This section discusses the effective use of technology for small cases for certain phases of the Electronic Discovery Reference Model.[83]

A. Collections

With multiplying data types and data sources for collection, this area of eDiscovery offers a wide variety of technologies. One application or software may collect some data sources or types, but no single technology collects all data types across all data sources. The varied data types and collection technologies add to the complexity of collecting data for small cases. This *Primer* does not include an exhaustive list of every possible collection type, source, and corresponding collection tool, but it is meant to provide practical tips and suggest technologies commonly used in small cases. The attached Appendix also provides a nonexhaustive list of various technologies that may be beneficial for eDiscovery needs in small cases.

---

83. *Electronic Discovery Reference Model* (2020), EDRM, https://edrm.net/resources/frameworks-and-standards/edrm-model/.

1. Reach agreement early as to data types, sources, and production format

All technologies have limitations regarding what data types they can collect. It is important to reach an agreement with the other parties regarding what is being collected and in what format it is being produced so that the appropriate collection technology can be used. This should be done to avoid producing data that is incomplete and may require an additional collection and review, which would be costly. Counsel should be wary of agreeing to collection and production formats for data with which they are unfamiliar or about which they have not consulted with their clients.

2. Do serial data requests seek unique, relevant information?

When the number of custodians increases, ESI volume balloons, so counsel should assess whether a potential custodian or data source includes unique content. If there are several custodians with the same role, consider collecting ESI from one key custodian before collecting from other custodians who may have the same or similar responsive content. This is also true for data sources. For instance, if a custodian mentions that she sent responsive emails from her phone after work hours, it is likely those emails are also stored on the mail server, making the collection of email from the phone duplicative. For each data source, ask if the source contains unique information or there is a more accessible source from which to collect the same information.

Issues of personal privacy make these considerations even more important. The data on an individual's mobile device generally includes significant personal data, including personal banking and health care information, social media, family photos, geographic tracking, and text messages. Collection of a

mobile device should be made only when the device contains unique information that is responsive to the document request.[84] If the information can be collected from another data source other than a personal mobile device, collection from that other source is recommended.

If collection from mobile devices is necessary, counsel should be aware of the cost and complexity and discuss the need with their clients. Mobile device software makers update operating systems and applications frequently, sometimes without the user's knowledge. Mobile device collection technology tools may not be capable of collecting from upgraded operating systems or applications. In practice, this means that a tool used to collect data from a mobile device may not behave consistently or work at all following operating system or other software upgrades.

Always check the collected data before production to confirm an appropriate collection, regardless of the collection method or tool.

3. Choose the collection method reasonable and proportional to the given matter

Text messages are commonly relevant in small cases. There are multiple ways to collect text messages that are reasonable and proportional to the needs of the case. The parties should agree to an appropriate collection method in advance.

Custodians may self-collect using screenshots or photos of messages, as long as the parties are aware that the images do not include metadata—such as when the message was sent or

84. *See, e.g.*, Lewis v. Archer Daniels Midland Co., No. CV 17-14190, 2018 WL 6591999, at *2 (E.D. La. Dec. 14, 2018) (stating that permitting forensic examination of personal cell phones must be weighed against inherent privacy concerns).

received—and agree to this form of production. Such images do not provide sender and recipient information unless the custodian provides these names with the production or the image contains the custodian's saved name for the other text participants. Group messages with multiple text participants may require that the custodian manually identify each participant in each image of the messages. This collection method may be cumbersome for the custodian, depending on the number of messages to be produced, and may subject the custodian to questions regarding the method of collection. These questions may implicate the chain of custody, or make authentication difficult or impossible.[85] In some circumstances, a neutral nonparty mobile device forensic expert may be worth the cost, even in a small case. The use of forensic vendors is discussed further below.

Another option for collecting text messages is iMazing, an application that can be used to view, save, and print messages from mobile devices. The cost of the iMazing application is minimal, especially compared to the cost of forensic collection of a mobile device for extracting and producing text messages. Use of this application or others like it still requires the custodian to self-collect or collect with the assistance of counsel, but the process is much less cumbersome. Beware that these applications may not extract all information, such as images or photos that are sent via text message. The collection and subsequent production may be incomplete if nonextracted information is responsive to the document request. It is important to understand the limitations of collection tools and discuss these with opposing counsel so that an agreement can be reached regarding the format of the data being produced.

85. *See Commentary on ESI Evidence & Admissibility, Second Edition*, *supra* note 74.

If custodians use cloud backup for their mobile devices, they may be able to log into their cloud storage account to collect the requested data, including text messages. The timing of the storage backup is key for this collection method. This method likely involves custodial self-collection unless the client provides counsel or an eDiscovery technology provider with access to its cloud account.

If a more comprehensive approach is needed, the use of a forensic collection tool or vendor such as Cellebrite may be necessary. Cellebrite is a forensic collection tool that will extract all information on a mobile device, including metadata. Purchasing Cellebrite is likely cost-prohibitive for a small case, but many vendors offer collections services using similar tools. Mobile device collection by vendors is typically billed either by hourly rate or on a per-device rate. If mobile device collection is warranted for a small case, seek a cost estimate from a provider for a forensically sound collection. If only certain data is needed from the device, independent forensic consultants may provide a more complete collection than a self-service application, such as PhoneView or the custodial screenshot method, while keeping costs lower than a complete mobile collection.

4. Some data source applications may contain their own extraction/collection capability

Some social media applications, such as Facebook and LinkedIn, include data extraction capability. These built-in tools require account access for self-collection by the custodian, but the resulting data may not be easy to review or produce because of the format in which it is downloaded. The screenshot or photo method discussed for text messages may also be employed for social media data, with the same caveats. Some social media sites include a separate messaging application, such as Facebook Messenger. It is important to understand what social

media applications the client uses and to explore whether those applications provide for a download of the data by the user.

If self-collection of social media is not possible or desirable, vendors offer sophisticated collection tools. X1 is one example of a collection tool for social media. As with Cellebrite, licensing X1 may be cost-prohibitive for one or two small cases, but vendors offer similar tools and social medial collection services. As with mobile devices, it is always a good idea to seek a cost estimate from a vendor with expertise in social media collection.

5. Be mindful of maintaining the original metadata when copying files

When collecting and copying files for production purposes, it is important to maintain the original metadata. Several collection tools help to maintain metadata without substantial cost. Robocopy is a free Windows utility accessible from the Windows command line (START → Windows System → Command Prompt → type "Robocopy" at the prompt). If counsel is guiding custodians through self-collection, the custodian can maintain metadata by "zipping" or compressing the files using common applications like 7-zip.

A common metadata collection pitfall causes the "Date Last Modified" field to change to the collection date. "Date" metadata fields for template files are also problematic, as the "Date Created" field reflects the date the template was created as opposed to the date the individual saved a new copy of the document. Counsel and clients should be mindful of changing metadata values like "File Path" and "File Name" when collecting data by copying or forwarding in email.

6. Be mindful of maintaining the original metadata when collecting emails

As discussed above, small cases do not always warrant forensic data collection. Custodial self-collection may be appropriate. When appropriate, counsel should guide custodians carefully as to collection methods. For instance, custodians should not forward emails to counsel for review. Doing so will change the metadata of the email, modifying the original "Sender," "Recipient," and "Date" fields. Rather, dropping emails as attachments into a new email, rather than forwarding them, is a useful way for counsel to collect the original emails. Forwarding sensitive emails and attachments may create data security risks as well, which goes beyond the scope of this *Primer*. Attention to data security is always critical when collecting sensitive or personal information.

Discussions of the collection and production format for cell phone, social media, and text message data are important. Cost is the primary driver in any plan to collect and produce these data types. Without planning, parties may have to re-collect and reproduce, increasing the overall discovery costs for the case.

B. Document Review, Analysis, and Production

1. Determine when an electronic discovery review tool is appropriate

Depending on the form of production, reviewing the collected data can be done in many ways. For instance, if the potential production comprises PDFs and a small number of images of documents, counsel may want to review simply by viewing the files in the application that created them. Under these circumstances, counsel may be able to review and produce using Adobe Acrobat to redact, Bates stamp, and print the production to PDF without incurring the expense of a vendor. It is

important to make sure that the redactions are permanent before producing or using the redacted document.

If the potential production set comprises several file types or a larger set of data, utilizing an electronic discovery review tool may be appropriate. This can be especially true for a requesting party who receives a large document production from a corporate defendant. Several cloud-based review tools are available on a monthly subscription or per-gigabyte cost basis. Some examples include Everlaw, Logikcull, and RelativityOne. While investing in an eDiscovery review tool may not be economically feasible for small cases individually, spreading or sharing the costs across multiple cases and multiple clients may have a significant cost-saving benefit. This is a growing industry, so practitioners are advised to research the current market for pay-as-you-go, no-commitment review tools. Small cases do not often require data analytics, but in the event counsel must search through large volumes of documents, some of these products can include advanced analytics tools that may also be useful. Such tools may help identify responsive documents more quickly than human review without unreasonably increasing the cost but may require more training to use.

For corporations with small cases, tools that are already licensed for purposes other than discovery might have capabilities that also support litigation. One example is Office 365, which has electronic discovery capabilities for some license levels. Consult with the corporate Microsoft representative or information governance partner to discuss whether the Microsoft license allows collection, review, analysis, and production of data without the need to export to a non-party vendor.

2. When applying redactions, be mindful of embedded images and metadata

Unless the parties agree that metadata production is not required, be careful that redacted material is not produced inadvertently. This can happen in several ways. When a non-email document contains embedded images, such as a screenshot from another application, the embedded image or screenshot is extracted as a child to the parent e-file. When applying redactions to a parent document that includes an embedded image, remember to redact the child image document if it contains material that should not be produced. Similarly, when applying redactions to imaged files (PDFs or TIFFs of native files), remember that any redacted text must also be removed from a separate metadata or text file. Otherwise, the information redacted from the image may be inadvertently produced. For those unaccustomed to producing documents with text or load files, consult with an expert to quality-check production redactions. Several new tools on the market offer "auto-redaction" of data such as Personally Identifiable Information.

3. Determine production format early

This *Primer* does not recommend any specific ESI protocol or form of production but does provide some tips and caveats for productions in small cases.

- Acrobat DC Pro can be used to Bates stamp and redact productions.
- Produce documents in a readable form. Produce each document as a discrete image file instead of combining multiple, individual documents into a single large PDF document.
    - The most common production format is a TIFF image, but some file types are better suited for a native production (for

definitions of these production formats as well as other electronic discovery related definitions, please see *The Sedona Conference Glossary*).[86]

- Excel spreadsheets and PowerPoint presentations are examples of file types that are commonly produced natively. When a single Excel spreadsheet is imaged, it can result in hundreds or thousands of pages, with columns and rows spanning multiple pages, making it not readily readable. Thus, these file types are typically produced natively even if they require redactions.
- PowerPoint presentations are also often produced natively to maintain slideshow effects. Once the presentation is imaged, any animations or special features incorporated into the presentation are no longer viewable. While there may not be a one-size-fits-all approach when it comes to production format, it is important to discuss production format along with data types and sources during the 26(f) conference as outlined above.

86. *The Sedona Conference Glossary: Fifth Edition*, *supra* note 22.

VII. CONCLUSION

While small cases may not suffer from the myriad complexities of large-scale litigations, small case discovery can still be complex, as explored in this *Primer* and illustrated by the efforts to develop it. While some of the tips outlined above apply to cases of any size, they are all particularly helpful in small cases where prevailing standards of proportionality, reasonableness, and cooperation must be applied to the management of ESI and discovery processes. This *Primer* is meant to be a tool to aid in the process of fulfilling Rule 1's duty of a "just, speedy and inexpensive determination" when it comes to fulfilling discovery obligations in small cases.

APPENDIX[87]

I. Collection Software

A. Text Messages: Screenshots and Merge Together

Parties may consider collecting and producing text messages by taking screenshots of the messages and using an app like Tailor or Stitch It to combine and render them in a readable form. This is not a forensic collection, and metadata of the original message will be missing from the collection. This is a self-collection method that relies on the owner of the phone to do the heavy lifting of identifying and collecting responsive text messages but that should be completed under the supervision or guidance of counsel. This approach may address concerns about disclosure of irrelevant personal data. It is important to document the time and date of the screenshots and verify the underlying information (e.g., participant/contact information, date and time information). The following two videos show how to best utilize this method:

- iPhone
- Android

B. Phone Collections: Apps or Software for your iPhone or Android

iMazing is another product that that can be used in collecting text messages or other phone data. This is software installed on a Windows or Mac computer. When an iPhone/iPad is connected to the computer, it allows the user to search and filter messages that can be exported to a TXT or PDF file.

87. The Appendix is neither exhaustive nor an endorsement of any particular technology or provider. It includes a sampling of available tools and technologies for illustrative purposes only.

This blog post from iMazing describes how to use the product for legal purposes. The software is around $50 for a single license.

For Android devices, similar products such as SMS Backup & Restore or Dr. Fone export messages as CSV files.[88]

Below is a list of various technologies depending on the phone at issue:

- iPhone: "Decipher TextMessage," "Keepster," "iMazing," "iTunes backup"
- Android: "SMS Backup & Restore Pro," "SMS Backup+," "Android Agent"

C. Cellebrite

Cellebrite is a leading tool for collecting mobile data. Cellebrite allows users to unlock devices by bypassing pattern, password, or PIN locks and overcome encryption challenges on both Android and iOS devices. In addition to extracting data from mobile phones, it also allows extraction from drones, SIM cards, SD cards, GPS devices and so on. Cellebrite can further utilize various recovery methods.

In addition, an examiner can use Cellebrite Physical Analyzer to generate a report in Cellebrite Reader format to share with others who do not have the software. This allows end users to review the data without the need for specialized Cellebrite software (which costs thousands of dollars) and to search, sort, filter, search within results, reorganize data within columns, and create customized tags that can be saved and reviewed

88. Enhanced or advanced Android messaging formats (*e.g.*, Rich Communication Service or "RCS") may not be supported by collections software, so parties should inquire into the capabilities and limitations of products—including forensic software—used to collect such formats when a custodian has enabled enhanced or advanced messaging.

later. End users can obtain a free copy of the Cellebrite Reader software either from the examiner or by creating a free account with Cellebrite.

D. X1 Social Discovery

X1 Social Discovery is a software tool for collecting and searching data from social networks and the internet. It aggregates comprehensive social media content and web-based data into a single user interface, collects metadata, and preserves the chain of custody. Unlike archiving and image capture solutions, X1 Social Discovery preserves information in searchable native format. Besides social media content, it is useful tool for collecting webmail and YouTube videos. This software works only with a PC operating system.

Both Cellebrite and XI Social Discovery are used by many eDiscovery providers, so in cases where it may not be cost-effective to license the tool directly, it may be cost-effective to reach out to a provider who is able to spread the software licensing costs across clients.

E. AnyDroid or Droid Transfer

Both AnyDroid and Droid Transfer allow users to remotely control content on an Android-based device. Both programs allow users to extract data, including text messages and call logs, from devices using the Android operating system. Because these are not forensic collection tools, there are limitations to the output of the data collected.

F. FTK Imager

FTK Imager is a free tool for previewing data and creating disk images. It offers searching capabilities, produces a case log file, and provides bookmarking and reporting features.

G. Magnet ACQUIRE

Magnet ACQUIRE lets digital forensic examiners quickly and easily acquire forensic images of a wide range of potential digital evidence sources, such as any iOS or Android device, hard drive, removable media, and cloud data. It supports both logical and physical acquisition. It is available at no cost to the forensic community.

H. Google Takeout

Google Takeout is a free tool used to export Google data for backup. It supports 51 types of data, including mail, drive content, calendars, browser bookmarks, and activity on YouTube. In essence, it retrieves and downloads all the information Google has about a user.

I. PinPoint Labs Harvester

Harvester is an eDiscovery collection software suite by Pinpoint Labs. This software allows searching, filtering, and copying files, folders, and documents from local and cloud environments. The collected data can be loaded into popular review platforms.

J. Paladin

Paladin and Paladin Toolbox allow various forensics tasks, including triage and imaging of drives, to be performed in a forensically sound manner.

K. Message Crawler

Message Crawler is an application that will convert data from numerous file formats to Relativity's "Short Message Format" (RSMF). Users can choose how data will be split, selecting either one day, one week or one month per conversation,

allowing them to see the data in the most convenient presentation for their needs.

L. Oxygen

Oxygen Forensics Suite is a forensic software that is used to acquire data from mobile devices, their backups and images, SIM card data, messenger logs, and cloud storage.

II. End-to-End Discovery Software

The following software are cloud-based, end-to-end eDiscovery solutions. The Sedona Conference does not recommend any solution over another. This list represents some of the many options that may be helpful in resolving eDiscovery needs in small cases.

- DISCO
- Everlaw
- LogikCull
- RelativityOne
- Reveal Data
- CasePoint
- NextPoint
- Lighthouse Spectra
- Zapproved ZDiscovery
- iConect
- CaseFleet
- GoldFynch
- Discovery Genie

III. General Software

A. Adobe Acrobat Pro

Adobe Acrobat Pro is a Portable Document Format (PDF) editor tool that allows users to view, create, search, edit, annotate, convert, redact, print, and manage PDF files. It is particularly useful in allowing text searches on otherwise nonsearchable PDFs (typically PDFs that are scanned paper) by running Acrobat's optical character recognition process on the files. Making PDFs searchable assists users in identifying relevant information in a large set of PDF files. Being able to annotate and bookmark PDFs gives users the opportunity to more easily identify and find documents of particular interest and provides a basic means to organize these documents. It also has the ability to redact and bates stamp documents and create a PDF index to improve the ability to search multiple files at the same time. This software works with both PC and Mac operating systems.

B. Microsoft/Office365

Core eDiscovery in Microsoft 365 provides a basic eDiscovery tool that organizations can use to search and export content in Microsoft 365 and Office 365. Core eDiscovery can also be used to place an eDiscovery hold on content locations, such as Exchange mailboxes, SharePoint sites, OneDrive accounts, and Microsoft Teams. Nothing is needed to deploy Core eDiscovery, but there are some prerequisite tasks that an IT administrator and eDiscovery manager have to complete before Core eDiscovery can be used to search, export, and preserve content.

C. dtSearch

dtSearch is a search and retrieval program that is useful for searching discovery productions and viewing many different file types, including searchable PDFs, Microsoft files (Word, Excel, etc.), web data, and email. It includes a near-native viewer

that allows end users to search and view what a document looks like even when they don't have the associated application installed on their device (e.g., users can view a PowerPoint file even when they do not have PowerPoint on their computer). The program provides multiple ways of searching, including key word, fuzzy, and Boolean searching. This software works only with a PC operating system.

D. CaseMap/TimeMap/DocManager

CaseMap is a fact and case organization and analysis tool that allows users to track and organize case information regarding facts, persons, documents, and issues in one database. Documents relevant to the case are linked to the database, which allows end users to quickly search, sort, and filter case information. Various PDF reports, including fact chronologies, lists of persons, issues, and documents, can be easily produced to provide snapshots of critical case information. Users can embed into the PDF reports the source documents that have been linked to the database to allow sharing of key information with people who may not have access to the database.

TimeMap creates case-related visual timelines. The program allows users to create a variety of timelines useful for courtroom presentations and team and client meetings.

DocManager is a near-native image viewer specifically designed for CaseMap. It allows users to review and annotate documents linked to the database without having to open the source file, making it easier and faster to navigate through the documents.

E. ReadySuite

ReadySuite is a tool for creating and converting eDiscovery review database export and import files, including Relativity,

Ipro Eclipse SE, Summation, Concordance, and TrialDirector formats.

F. Beyond Compare

Beyond Compare is a data comparison tool that is useful for comparing and identifying differences between various files, including load files. It is helpful in identifying and syncing original and copy folders where the copy has failed (for example, due to overlong file names, or files sizes that are too large). It can do side-by-side comparison of directories (including FTP, SFTP, Dropbox, and Amazon S3 directories). This software works with both PC and Mac operating systems.

G. IrfanView

IrfanView is an image viewer that allows users to browse through images quickly or watch them as a slideshow. IrfanView also includes a photo editor, a batch file converter, and a scanner interface.

H. 7Zip

7Zip is a free, open-source file archiver used to compress or zip files secured with encryption. It is useful for reducing the file size and securing files when emailing.

I. Notepad++

Notepad++ is free software used for text and source-code editing.

J. Treesize

TreeSize Free is a free disk space manager for Windows that is used to display drive and folder sizes, including all subfolders, and to create reports on the findings. It allows users to sort files by fields such as file age and size.

K. Arsenal Image Mounter

Arsenal Image Mounter is a forensic disk image mounting solution that mounts the contents of disk images as shares or partitions, rather than complete, physical, or real disks.

L. PST Walker

PST Walker is an app that provides a portable PST viewer and data recovery for Microsoft Outlook. It is also used to restore corrupted or encrypted PST files and OST files.

M. Safecopy

Safecopy is a data recovery tool that is used to extract as much data as possible from a damaged source, such as floppy drives, hard-disk partitions, compact disks, and tape devices.

N. Foxit PhantomPDF

Foxit PhantomPDF Editor is similar to Adobe Acrobat Pro. It is software that lets users view, create, edit, comment, secure, organize, export, employ optical character recognition on, and sign PDF documents and forms.

THE SEDONA CONFERENCE COMMENTARY ON MANAGING INTERNATIONAL LEGAL HOLDS

A Project of The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6)

Author:

The Sedona Conference

Editor-in-Chief:

Ronni Dawn Solomon

Contributing Editors:

Franziska Fuchs
Brad Harris
Eric P. Mandel
Kimberly A. Quan
John C. Tredennick
Jennifer Tudor Wright

Steering Committee Liaison:

Hon. James C. Francis IV (ret.)

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 Managing International Legal Holds*, 24 SEDONA CONF. J. 161 (2023).

PREFACE

Welcome to the May 2023 final version of The Sedona Conference *Commentary on Managing International Legal Holds* ("*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 Ronni Solomon for her leadership and commitment to the project. We also thank Contributing Editors Franziska Fuchs, Brad Harris, Eric Mandel, Kimberly Quan, John Tredennick, and Jennifer Tudor Wright for their efforts, and Judge Jay Francis for his guidance and input as Steering Committee liaison to the drafting team. We thank Daryl Osuch for his contributions.

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
May 2023

TABLE OF CONTENTS

PREAMBLE

Parties in actual or anticipated cross-border litigation face a conundrum. On one hand, they are often required to comply with strict requirements for the preservation of discoverable data. On the other, privacy laws and regulations can severely restrict their legal ability to preserve personal data.

Although issues arise whenever preservation obligations and privacy requirements conflict, *The Sedona Conference Commentary on Managing International Holds* ("*Commentary*") focuses primarily on preservation obligations in the United States, because the U.S. arguably has the most comprehensive and significant preservation requirements of any country. Correspondingly, in discussing international data protection laws, the paper focuses mostly on the European Union's General Data Protection Regulation (GDPR)[1] because it is highly influential and has spurred, and continues to spur, similar regulations in other jurisdictions around the world.

While this *Commentary* will allude to other preservation and privacy regimes, it will not explore them in depth. By analyzing the application of GDPR in the context of U.S. preservation obligations, it sets out to provide a framework for counsel when applying international legal holds in any jurisdiction with conflicting data protection laws. It is hoped that readers will find it useful as they analyze and take steps to meet legal hold and data protection obligations.

---

1. 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. (L 119/1), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents [hereinafter GDPR].

I. INTRODUCTION

In 2007, The Sedona Conference Working Group 1 ("Sedona WG1") published for public comment the First Edition of *The Sedona Conference Commentary on Legal Holds: The Trigger & the Process*.[2] In 2010, Sedona WG1 released the final version,[3] which provided commentary and guidelines for the implementation and management of legal holds, with a primary focus on U.S. litigation and investigations.

In 2019, Sedona WG1 published *The Sedona Conference Commentary on Legal Holds, Second Edition: The Trigger & The Process*, which provided both an update on legal cases released after publication of the First Edition and commentary on the impact of the 2015 Amendments to the Federal Rules of Civil Procedure.[4] The Second Edition similarly focused on U.S. litigation and government investigations but added Guideline 12, which addressed the implications of preserving information located outside the United States:

> Guideline 12: An organization should be mindful of local data protection laws and regulations when initiating a legal hold and planning a legal hold policy outside of the United States.[5]

---

2. The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, Public Comment Version (Aug. 2007), *available at* https://thesedonaconference.org/publication/Commentary_on_Legal_Holds.

3. The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265 (2010).

4. The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341 (2019), *available at* https://thesedonaconference.org/publication/Commentary_on_Legal_Holds [hereinafter *Sedona Commentary on Legal Holds, Second Edition*].

5. *Id.* at 409.

The purpose of this *Commentary* is to expand on Guideline 12 by focusing on "international legal holds," defined as legal holds involving preservation obligations that cross international borders. The intent is to provide guidance and practice points for implementing international legal holds while at the same time complying with potentially conflicting international data protection laws and regulations (hereinafter "international data protection laws").

This *Commentary* does not focus on cross-border data transfers, which may become an important consideration when collecting data to preserve, or transferring data to another jurisdiction for analysis or review (e.g., outside of the European Union (EU), in the case of GDPR).[6]

The *Commentary* is written with several audiences in mind:

- U.S. companies and lawyers handling cross-border preservation issues in litigation or investigations;
- Non-U.S. lawyers or other legal professionals seeking to comply with U.S. preservation obligations or other jurisdictions' preservation requirements and, at the same time, data protection requirements in their own or other countries;
- Judges addressing whether, how, and under what circumstances parties should be required

6. GDPR articles 44 to 50 govern the transfer of data outside of the EU and require separate justification before the data can be transferred. *See, e.g.*, The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, 17 SEDONA CONF. J. 397 (2016); Guidelines 05/2021 on the Interplay between the application of Article and the provisions on international transfers as per Chapter V of the GDPR at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en (last visited May 19, 2023).

to preserve information where conflicts with international data protection laws are unavoidable;[7]

- Government agencies and authorities seeking the preservation of information stored in other jurisdictions; and
- Data protection authorities so they might better understand an entity's good-faith efforts and attempts to achieve compliance.

7. *See, e.g.*, The Sedona Conference, *Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders*, 21 SEDONA CONF. J. 393 (2020).

II. PRESERVATION AND INTERNATIONAL DATA PROTECTION REQUIREMENTS

A. Preservation Obligations: The Duty to Preserve

In 2003, U.S. District Court Judge Shira Scheindlin set the stage for a new era in United States litigation when she stated in *Zubulake v. UBS Warburg*:

> Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents.[8]

Judge Scheindlin's admonition sprang from the longstanding common-law duty for litigants to prevent spoliation—the loss or destruction of relevant materials that may later be used by another at trial.[9] It also flowed from the principle of broad pretrial disclosure in the U.S. first established in 1938 and continuing through the promulgation of the Federal Rules of Civil Procedure.[10]

---

8. Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

9. *The Sedona Conference Glossary* defines spoliation as: "The destruction of records or properties, such as metadata, that may be relevant to ongoing or anticipated litigation, government investigation, or audit." *The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition*, 21 SEDONA CONF. J. 263, 373 (2020), *available at* https://thesedonaconference.org/publication/The_Sedona_Conference_Glossary. *See also* Robert Keeling, *Sometimes Old Rules Know Best: Returning to Common Law Conceptions of the Duty to Preserve in the Digital Information Age*, 67 CATH. U. L. REV. 67 (2018) (historical background of common law duty to preserve and comparing application of today's standard).

10. Fed. Judicial Ctr., *Federal Rules of Civil Procedure Establish Uniformity* (Sept. 16, 1938), https://www.fjc.gov/history/timeline/federal-rules-civil-procedure-establish-uniformity. Many states in the U.S. have adopted rules

In the years since *Zubulake IV*, many U.S. organizations have established procedures and practices to enable the preservation of information—whether hard-copy documents, electronically stored information, or other evidentiary materials that may be subject to a discovery obligation (hereinafter "discoverable information")—through the implementation of a legal hold.[11] While the terms "litigation hold" and "legal hold" are often used interchangeably, this *Commentary* uses the broader term "legal hold" to encompass government investigations as well as civil litigation.[12]

Thus, U.S. organizations and others subject to U.S. civil litigation are required to preserve discoverable information when they "reasonably anticipate" litigation or an investigation.[13] To comply with U.S. preservation obligations, an organization will need to consider taking a number of steps. These may include (1) sending a written legal hold notice to individuals likely to be the custodians of discoverable information; (2) suspending routine deletion or destruction policies for discoverable

---

modeled on the Federal Rules of Civil Procedure and allow broad pretrial discovery.

11. This *Commentary* uses the phrase "discoverable information" consistent with the *Sedona Commentary on Legal Holds, Second Edition*, *supra* note 4, at 348. The authors recognize that information deemed to be relevant may vary from case to case, especially in civil litigation, where some parties may take a narrower position, versus governmental investigations, where relevancy can be very broadly construed. The goal of this *Commentary* is to help practitioners and others navigate between even the most demanding legal hold obligations and privacy protections. The authors also note that the more demanding the preservation obligation, the stronger the argument is for meeting the necessity requirement imposed by the GDPR and similar rules. *See infra* Section II.C.2.a.

12. *See In re* Delta/Airtran Baggage Fee Antitrust Litig., 770 F. Supp. 2d 1299, 1307–08 (N.D. Ga. 2011) (recognizing that preservation obligations apply to government investigations).

13. *Zubulake IV*, 220 F.R.D. at 218.

information; (3) adopting "preservation in place" strategies to suppress manual alteration or deletion within systems that hold discoverable information; and (4) copying sources to a centralized location to ensure the information will be available during the discovery process. The legal framework and guidelines for compliance with U.S. preservation obligations are detailed in *The Sedona Conference Commentary on Legal Holds, Second Edition*.[14]

Failing to meet U.S. preservation obligations may lead to sanctions, including curative measures and sanctions such as instructing the jury to presume that the information was unfavorable to the party that failed to meet its preservation obligation, monetary payments, or even dismissal of the action or the entry of a default judgment.[15] It also may include civil tort liability and criminal penalties for destruction of evidence.[16]

Non-U.S. Preservation Obligations: In non-U.S. jurisdictions, the extent of preservation obligations often turns on whether the jurisdiction follows common law or civil law and whether the matter relates to a private civil matter or a governmental investigation.[17] For example, common law countries such as the United Kingdom, Canada, Australia, and New

14. *See Sedona Commentary on Legal Holds, Second Edition, supra* note 4.

15. *See* FED. R. CIV. P. 37(e).

16. 18 U.S.C. § 1519.

17. *See* Kenneth N. Rashbaum, Matthew Knouff & Melinda C. Albert, *U.S. Legal Holds Across Borders: A Legal Conundrum?*, 13 N.C.J.L. & TECH. 69, 85 (2011), *available at* https://www.bartonesq.com/wp-content/uploads/2014/05/UNC-JOLT-Art_Rashbaum_Knouff_Albert_69_94.pdf. *See also* The Sedona Conference, *Framework For Analysis Of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery*, Public Comment Version (2008), at 14–16, *available at* https://thesedonaconference.org/publication/Framework_for_Analysis_of_Cross-Border_Discovery_Conflicts.

Zealand recognize an obligation to preserve relevant documents in the context of civil litigation and investigations.[18] In the UK, a party is required to preserve and disclose all documents on which it relies as well as those that adversely affect its case or support another party's case.[19] As set forth in UK Civil Procedure Rule Practice Direction 31B.7, "[a]s soon as litigation is contemplated, the parties' legal representatives must notify their clients of the need to preserve disclosable documents. The documents to be preserved include Electronic Documents which would otherwise be deleted in accordance with a document retention policy or otherwise deleted in the ordinary course of business."[20]

Civil law countries impose more limited preservation obligations. For example, German procedural rules, while not imposing a direct obligation to preserve, allow for the ease of evidentiary rules in cases where documents can no longer be

18. *See* James A. Sherer & Taylor M. Hoffman, *Cross-border Legal Holds: Challenges and Best Practices*, PRACTICAL LAW 28 (Oct./Nov. 2017), *available at* https://www.bakerlaw.com/webfiles/Litigation/2017/Articles/10-17-2017-Sherer-FeatureCrossBorder.pdf.

19. UK CPR 31.6.

20. UK CPR Practice Direction 31B.7. *See How Relevant is Legal Hold to the UK Market?*, CYFOR, https://cyfor.co.uk/how-relevant-is-legal-hold-to-the-uk-market/ (last visited May 19, 2023).

produced.[21] France and Spain, similarly, have limited preservation obligations.[22]

In such jurisdictions, the absence of a duty to preserve evidence may create legal and cultural conflicts if the individual or legal entity is required to preserve evidence by another jurisdiction such as the U.S.[23]

B. International Privacy Requirements: The Rights of Individuals

A growing number of jurisdictions recognize that individuals have a fundamental right to privacy. Many have enacted data protection laws that protect the rights of natural persons by restricting the collection, use, storage, or alteration of their personal information.[24] In most cases, these laws restrict the

---

21. As a rule, the parties provide documents they will rely on to support their case in their trial briefs, including the opponent's documents. Where a requesting party relies on a producing party's document to support its brief, the requesting party can move the court for an order compelling the producing party to produce the document to the court. ZIVILPROZESSORDNUNG [ZPO] [CODE OF CIVIL PROCEDURE] art. 425. Where the producing party cannot or does not produce the document to the court, the court can either accept a copy of the document provided by the requesting party as sufficient or can accept the requesting party's characterization of the contents of the document as evidence. *Id.*, art. 427. The preservation of documents is therefore in the interest of the parties.

22. *See, e.g.*, Olivier de Courcel, *The e-Discovery and Information Governance Law Review: France*; and Enrique Rodríguez Celada, Sara Sanz Castillo & Reyes Bermejo Bosch, *The e-Discovery and Information Governance Law Review: Spain*, THE E-DISCOVERY AND INFORMATION GOVERNANCE LAW REVIEW (Jennifer Mott Williams ed., 3d ed. 2021), https://www.uria.com/documentos/colaboraciones/2997/documento/Spain-ds.pdf?id=12322_en.

23. *See Cross Border Investigations Update, Legal Holds in Cross-Border Investigations*, SKADDEN (Aug. 2018), https://www.skadden.com/insights/publications/2018/08/cross-border-investigations-update#legal.

24. GDPR, *supra* note 1, art. 1 (*Subject-matter and objectives*); *id.* at art. 4(1).

transfer of personal information to jurisdictions that fail to provide adequate levels of protection.

Personal Data: The GDPR is an influential and prominent example of a comprehensive data protection law[25] that protects the rights of individuals with respect to their personal information. The GDPR took effect on May 25, 2018, and is binding on all Member States of the European Union[26] as well as the Member States of the European Economic Area (EEA).[27] Under the GDPR, "'personal data' means any information relating to an identified or identifiable natural person ('data subject')."[28] It is broadly defined and includes anything that can be categorized as "individual information." For example, it includes information that shows the relationship of a person to his or her environment, objects, or third parties, as well as his or her financial situation (assets, salary, creditworthiness), contractual relationships, friendships, ownership, consumption or communication behavior, working hours, email addresses, and so on.[29] It

25. The GDPR replaced the 1995 Data Protection Directive. The GDPR established the European Data Protection Board (EDPB), which contributes to the consistent application of data protection rules throughout the EU. *See* European Data Protection Board, *Who we are*, https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en. The EDPB's predecessor was the Article 29 Working Party. The work of the Article 29 Working Party resulted in the development of the GDPR.

26. *See* GDPR, *supra* note 1, art. 99 (*Entry into force and application*), *id.* at Art. 3 (*Territorial scope*).

27. Specifically, Iceland, Norway and Liechtenstein.

28. *Id*.

29. Case C-342/12, Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT), 2013 European Court of Justice, https://curia.europa.eu/juris/document/document.jsf?text=&docid=137824&page.Index=0&doclang=EN&mode=req&dir=&occ=first&part=1. *See also* BORIS PAAL & DANIEL A. PAULY, DATENSCHUTZ-GRUNDVERORDNUNG BUNDESDATENSCHUTZGESETZ: DS-GVO BDSG, 3. Auf. (2021), Art. 4, Rn. 14.

also includes the data subject's name, age, origin, gender, education, marital status, address, date of birth, eye color, fingerprints, genetic data, state of health, photographs and video recordings, personal beliefs, preferences, behaviors, or attitudes.[30] Likewise, personal information also applies to both content and metadata such as IP (internet protocol) addresses, cookies, or radio frequency identifiers.[31] Even where a subject's identity has been replaced by a pseudonym, the information is still considered personal information.[32]

The key point is that data subjects have protected rights under the GDPR regarding the use of their personal information—regardless of whether the personal data in question relates to their private life or is part of their employer's business documents.[33] Hereafter, the terms "personal information" and "personal data" are used interchangeably.[34]

Processing: Under the GDPR, organizations must process personal information lawfully, fairly, and in a transparent manner as it relates to the data subject.[35] "Processing" is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation,

30. *Id.*

31. *Id.*, Art. 4, Rn. 18.

32. GDPR, *supra* note 1, Recital 26, https://gdpr-info.eu/recitals/no-26/.

33. SPIROS SIMITIS, ET AL., DATENSCHUTZRECHT, 1. Auf. (2019), Art. 88, Rn. 1.

34. The reader should be mindful, however, of personal information that, because of its sensitivity, requires a higher degree of protection. Unless the context otherwise makes it clear, that information is not the subject of the paper.

35. GDPR, *supra* note 1, art. 5(1)(a).

use . . . ."[36] It also includes holding onto personal information after it should have been deleted.[37] Most relevantly to this *Commentary*, it includes the preservation of documents in connection with a legal hold.[38]

Controllers and Processors: To protect data subjects' rights, the GDPR focuses on "controllers" and "processors." Controllers are organizations or individuals that make decisions over the how and why of the processing of personal data.[39] Processors are organizations or individuals that process information on behalf of, and under the instructions of, controllers.[40]

A controller would include a company processing personal data on its internal information technology (IT) systems for purposes of its business. A processor could be any IT service provider to whom the company has outsourced processing tasks, such as a hosting provider, a records management company, a customer hotline, or an employee benefits company.

Extraterritorial Jurisdiction: The GDPR asserts extraterritorial jurisdiction. It applies to controllers and processors who are established or doing business in the EU regardless of whether

---

36. *Id.*, art. 4(2).

37. *See, e.g., id. a*rt. 17 (*i.e.*, right to be forgotten).

38. *See, e.g., id.*, art. 4(2); this was also true prior to the adoption of the GDPR. *See* Working Document 1/2009 on pre-trial discovery for cross border civil litigation, adopted on Feb. 11, 2009, 00339/09/EN WP 158, *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf. (Under Directive 95/46, any retention, preservation, or archiving of data for such purposes would amount to processing.).

39. *See e.g.*, GDPR, *supra* note 1, art. 4(7), which defines a controller as a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal information."

40. *See id.*, art. 4(8), which defines a processor as a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." A "controller" can also be a "processor."

they process any personal information in the EU or elsewhere.[41] It also applies to controllers and processors located outside the EU if they offer goods or services to people who are "in" the EU or who are monitoring the behavior of persons in the EU.[42]

Penalties and Sanctions for Violations: Failing to comply with the GDPR's requirements may expose a controller or processor[43] to severe monetary penalties—up to 20 million Euros or 4 percent of the violator's worldwide annual gross revenue for the prior year, whichever is higher.[44] Violators may also be subject to nonmonetary administrative sanctions and may be required to pay compensation to data subjects whose rights have been violated.

C. Preservation Under the GDPR

Two GDPR provisions govern the implementation of preservation steps. First, preservation must comply with Article 5, which sets out a series of guiding principles that govern all processing of personal information.[45] Second, preservation must comply with Article 6, which sets out requirements that must be

41. *See id.*, art. 3(1).

42. *Id*. at art. 3(2) and 3(3). Recital 25 clarifies that Article 3(3) refers to those places which, according to international law, are not subject to the third country in which they are geographically located. These are in particular the diplomatic or consular representations of a Member State in a foreign country outside the European Union. This third scenario is unlikely to occur in the legal hold context and is therefore not discussed further.

43. *See id*., art. 4(8).

44. *Id.*, art. 83(5).

45. *Id.* at art. 5(1)(a-f).

followed to make processing lawful.[46] A party must satisfy both provisions in order to preserve information lawfully.[47]

1. Meeting Article Five's Guiding Principles

Article 5, Paragraph 1 sets forth "Principles relating to the processing of personal data," stating that personal information shall be:

a. Processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ("purpose limitation");
c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
d. Accurate and, where necessary, kept up to date ("accuracy");
e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information are processed; ("storage limitation"); and
f. Processed in a manner that ensures appropriate security of the personal information, ("integrity and confidentiality").

46. *Id*. at arts. 7–8, 9–11, and 12–23.

47. European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, at 3 (adopted 25 May 25, 2018), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

The controller is further responsible to demonstrate compliance with these principles when processing such data ("accountability").[48]

Although described as "principles," these provisions are in fact binding regulations applicable to controllers and processors and apply to every aspect of processing, including the preservation of personal information and implementation of legal holds.[49] Most importantly, they shape and inform all other provisions of the GDPR.[50] A violation of these principles makes the data processing unlawful and exposes the wrongdoer to potentially severe sanctions.[51]

Although each must be considered carefully, several of the principles are particularly important in the context of implementing preservation steps for a U.S. legal hold:

Lawfulness: Data processing is permitted under certain conditions set out in the GDPR. The permissible conditions are based on weighing the data subject's fundamental human right to data protection against the lawful, legitimate purpose, interest, and obligations of the controller.[52] Establishing a lawful basis under Article 6, explained in more detail below, is a prerequisite for processing in the context of a legal hold.

Transparency: The principle of transparency is an essential principle related to the processing of information. It does not

48. *See* GDPR, *supra* note 1, art. 5(1)(a-f) (paraphrased in part).

49. PAAL & PAULY, *supra* note 2, Art. 5, Rn. 1.

50. Alexander Roßnagel, in: SIMITIS, ET AL., *supra* note 33, Art. 5 Rz. 15.

51. GDPR, *supra* note 1, art. 83(5)(a).

52. *See* Charter of Fundamental Rights of the European Union, Art. 8, 2012 O.J. (C 326) 391 (26 Oct. 2012), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN (establishing the fundamental rights of the data subject); *See also,* GDPR, *supra* note 1, art. 5 (principles relating to the processing of personal data).

merely imply a right for the data subject to request information.[53] It also includes the obligation of the controller to actively provide the data subject with all information necessary to enable the data subject to verify whether processing is lawful and to exercise his or her rights.[54] Without sufficient transparency, the data subject is effectively deprived of his or her fundamental human rights.[55] Therefore, where a controller collects personal information from a data subject, it is obliged, even without a data subject requesting it, to inform the subject that data is being collected and the purpose and effect of the collection.[56] The principle of transparency also requires that information and communication relating to the processing of personal information be easily accessible and easy to understand, and that clear and plain language be used.[57]

Purpose Limitation: Information may only be processed for specific, explicit, and legitimate purposes.[58] It may not be processed for abstract or general purposes nor retained for its potential future value and use to the controller. Processing for unspecified purposes is specifically prohibited.[59] A legitimate purpose must be identified when or before processing occurs. When there is no longer a legitimate purpose for such processing, the personal information must be deleted.[60]

---

53. *Id.*, art. 12.

54. *Id.,* Recital 39 (Principles of Data Processing); Roßnagel, in: SIMITIS ET AL., *supra* note 33, Art. 5, Rz. 50.

55. *Id*.

56. *See* GDPR, *supra* note 1, Recital 39.

57. *Id.*

58. *Id.*, art. 5(1)(b); Roßnagel, in: SIMITIS ET AL., *supra* note 33, Art. 5, Rz. 69.

59. *Id*. at Rz. 72.

60. *See* GDPR, *supra* note 1, art. 17 (*Right to erasure ('right to be forgotten')*).

Minimization: Data minimization describes a means-ends relationship: information may only be processed to the extent necessary to achieve the defined purpose for data processing.[61] This requirement limits the extent and depth of processing and thus minimizes the impact on the data subject's right to data protection. This principle also requires that the purpose be specified and pursued in a way that ensures as little personal information as possible is processed.[62] Additionally, the period for which personal data is stored is limited to the strict minimum.[63]

The principle does not call for a minimization of information per se. Rather, it is designed to reduce the potential harm and impact on a data subject's rights by reducing the amount of personal information processed or disclosed to what is unavoidably necessary.

Accountability: Under the accountability principle, the controller is responsible for, and must be able to demonstrate compliance with, Article 5.[64] The controller must actively take measures to implement the principles in its data processing operations. The controller must also document its actions and be able to prove compliance with the obligation.

2. Establishing a Lawful Basis under Article Six

Article 6 begins with the unambiguous and fundamental statement: *"Processing shall be lawful only if and to the extent that*

61. *Id.*, art. 5(1)(c); Bernard Marr, *Why Data Minimization Is An Important Concept In The Age of Big Data*, FORBES (Mar. 16, 2016), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/?sh=3ceb8bc41da4.

62. Roßnagel, in: SIMITIS ET AL., *supra* note 33, Art. 5, Rz. 123.

63. GDPR, *supra* note 1, Recital 39.

64. *See* European Data Protection Supervisor, *Accountability*, https://edps.europa.eu/data-protection/our-work/subjects/accountability_en (last visited May 19, 2023).

one of the following applies." It then proceeds to enumerate six bases for lawful processing. The following are the most commonly considered in conjunction with preservation: (a) the legitimate interests of the controller or a third party, (b) consent of the data subject, and (c) compliance with a legal obligation.

(a) Pursuing a Legitimate Interest: The most common avenue for establishing a lawful basis for preserving personal information is pursuing a legitimate interest of the controller. The relevant GDPR provision provides:

> processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[65]

This provision requires the controller to show: (1) the controller's legitimate interest, (2) that the processing (preservation) is necessary to protect that interest, and (3) that the interest is not outweighed by the fundamental rights and freedoms of the data subject.

The threshold for showing what constitutes a controller's legitimate interest depends on the circumstances.[66] For example, defending or asserting a U.S. legal claim may be able to meet that threshold.[67] The mere possibility, however, of a U.S. legal proceeding, as opposed to reasonable anticipation of one, is not alone sufficient.[68]

---

65. GDPR, *supra* note 1, art. 6(1)(f).

66. Working Doc. 1/2009, *supra* note 38.

67. *Id*. at 2.

68. *Id*. at 8, 13 ("There may however be a further difficulty where the information is required for additional pending litigation or where future

The second factor that a controller must show—necessity—limits the extent of the processing to the defined purpose (e.g., defense of a legal claim). Processing may be deemed necessary if no less intrusive, but equally effective, means is available.[69]

The third factor requires that once a legitimate interest and the requisite necessity have been established, the controller must show that its preservation requirements are not overridden by the interests of the data subject. As the Article 29 Working Party stated:

> Against these aims have to be weighed the rights and freedoms of the data subject who has no direct involvement in the litigation process and whose involvement is by virtue of the fact that his personal data is held by one of the litigating parties and is deemed relevant to the issues in hand, e.g. employees and customers.[70]

Thus, the controller must demonstrate that preservation is not outweighed by the interests of the data subject.[71] Issues to be considered include:

---

litigation is reasonably foreseeable. The mere or unsubstantiated possibility that an action may be brought before the U.S. courts is not sufficient.") ("However, the Working Party reiterates its earlier opinion that Art. 26 (1)(d) of the Directive cannot be used to justify the transfer of all employee files to a group's parent company on the grounds of the possibility that legal proceedings may be brought one day in U.S. courts.").

69. Schaffland/Holthaus, in: HANS-JÜRGEN SCHAFFLAND & NOEME WILTFANT, DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)/BUNDESDATEN SCHUTZGESETZ (BDSG), Art. 6, Rn. 117c.

70. Working Doc. 1/2009, *supra* note 38, at 9; *See also* Art. 29 Working Party Working Document on surveillance of electronic communications for intelligence and national security purposes (WP228), at 9 (adopted Dec. 5, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf.

71. Working Doc. 1/2009, *supra* note 38, at 9–10.

- The relevance of the preserved information to the matter;
- The consequences of preservation to the data subject; and
- The proportionality of the preservation efforts.

Ultimately, as the Article 29 Working Party stated: "The personal data must be adequate[,] relevant and not excessive in relation to the purposes for which they are collected and/or further processed."[72]

(b) Consent: Under Article 6(1)(a), a data subject may consent to the processing (in this case, preservation) of his or her personal information for one or more specific purposes.[73] Recital 32[74] and Article 7[75] set forth conditions for consent[76] and require that it be:

- in writing;
- explicit and freely given (without pressure or influence);
- unambiguous;
- fully informed and include the right to withdraw; and
- given specifically for each specific matter requiring preservation.[77]

---

72. *Id*. at 10.

73. GDPR, *supra* note 1, art. 6(1)(a).

74. *Id.*, Recital 32.

75. *Id.*, art. 7.

76. *See also* Guidelines 2/2018, *supra* note 47, at 6–8.

77. A data subject must be informed in accordance with GDPR Article 13 information, which is to be provided where personal information is collected from the data subject.

In addition, the controller must provide the individual with information about why the data is being collected or preserved, the specific legal basis the controller is relying on for preservation, and how to contact a data protection officer to lodge an objection.[78] Ultimately, the controller has the burden to demonstrate that these elements have been established.[79]

There are several risks to relying on consent as a lawful basis for preservation under the GDPR. First, data protection agencies and courts are reluctant to find that an employee can freely give consent to his or her employer because of the power imbalance inherent between employers and employees.[80] Valid consent between an employee and employer can be difficult to establish.[81]

---

78. GDPR, *supra* note 1, art. 13(1)(b-c).

79. *Id.*, Recital 42; Art. 7(1).

80. Winfried Veil, *Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis*, 71 NEUE JURISTISCHE WOCHENSCHRIFT, No. 46, 3337 (2018).

81. *See* SIMITIS, ET AL., *supra* note 33, Art. 88, Rn. 12. Because of this structural imbalance, employees are typically not in a position to achieve adequate protection of their personal data in the employment relationship by means of private autonomy. A particularly clear example of this is the consent of employees to the processing of their data by the employer, the voluntariness of which is often likely to be lacking if it is only given in the interests of the employer. Consequently, the national German data privacy law restricts the permissibility of employees giving their consent to the processing of their data in Section 26 (2) BDSG: "If the processing of personal data of employees is based on consent, the assessment of the voluntariness of the consent shall take into account in particular the dependency of the employee in the employment relationship and the circumstances under which the consent was given. Voluntariness may exist in particular if a legal or economic advantage is achieved for the employed person or the employer and the employed person pursue similar interests. Consent must be given in writing or electronically, unless another form is appropriate due to special circumstances."

Second, under the GDPR, a data subject can revoke his or her previously given consent at any time.[82] While revocation of consent does not make previous preservation activities unlawful, it might limit preservation options for the same information in the future. Future preservation could violate the GDPR even if an alternative lawful basis were otherwise available.[83]

Third, obtaining consent simply may not be feasible. Certain documents may contain personally identifiable information of a number of individuals (e.g., an email conversation between several persons) and would require consent from all of them. While obtaining consent within a single organization may be an option, obtaining consent of data subjects such as former employees, customers, or suppliers will likely be difficult.

(c) Compliance with a Legal Obligation: Implementing preservation steps to comply with a legal obligation would seem to be another possible lawful basis under Article 6.[84] The phrase "legal obligation" under the GDPR, however, is expressly limited to an obligation that arises out of EU law or the law of an EU Member State.[85] As a result, this basis is largely

82. GDPR, *supra* note 1, art. 7(3); *see* GDPR Recital 43.

83. Consent cannot easily be replaced with an alternative basis at a later time. "Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements." UK INFORMATION COMMISSIONERS OFFICE, GUIDE TO THE GENERAL DATA PROTECTION REGULATION (GDPR) [hereinafter UK GUIDE TO GDPR], *Lawful basis for processing*, at 53, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ (last visited May 19, 2023).

84. *See* GDPR, *supra* note 1, art. 6(1)(c).

85. *Id*. at Arts. 6(3) and 6(1)(f).

inapplicable when preservation obligations arise pursuant to the laws of a non-EU jurisdiction.[86]

D. Jurisdictions Adopting Data Protection Regimes Similar to GDPR with Preservation Restrictions

Other nations have followed the EU's approach and adopted similar data protection laws. Below are examples of these laws, highlighting similarities and potential differences with the GDPR. These examples specifically focus on whether implementing preservation steps under a U.S. legal hold would potentially violate various data protection laws.

1. Europe: Non-EU Nations

United Kingdom: After leaving the EU, the UK enacted its own data protection law ("the UK GDPR"), which is substantively similar to the GDPR.[87] Like the GDPR, the UK GDPR's definition of "processing" includes any set of operations performed on data, including the mere storage, preservation, hosting, consultation, or deletion of the data.[88] Accordingly, it is

86. There may be instances where international treaties exist, such as the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (Hague Evidence Convention), that apply in a specific matter. In cases where a requesting party successfully serves the opposing party under the Hague Evidence Convention, that party may then be subject to preservation rules imposed on it by its own jurisdiction. However, some signatory states, such as Germany, have objected in part or fully to application to pretrial discovery through an objection according to Article 23, thus making it inapplicable in the context of a legal hold.

87. For a redline of the changes from EU GDPR to UK GDPR, see the General Data Protection Regulation Keeling Schedule, *available at* https://uk-gdpr.org/wp-content/uploads/2022/01/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

88. DLA Piper, *Collection and Processing: United Kingdom,* DATA PROTECTION LAWS OF THE WORLD, https://www.dlapiperdataprotection.

likely that implementing a U.S. legal hold involving personal information collected from natural persons who are located in the UK would be considered data processing under the UK GDPR and require the controller to comply with that law.[89] The UK 2018 Data Protection Act, which enables the application of the EU GDPR in the UK, continues to supplement the UK GDPR.[90]

Switzerland: Switzerland is not an EU Member State but has its own data protection law called the Swiss Federal Act on Data Protection ("FADP"). It provides similar rights to those afforded by the GDPR.[91] The FADP defines processing as "any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data."[92] This is

---

com/index.html?t=collection-and-processing&c=GB (last modified Jan. 27, 2021).

89. UK GDPR is nearly identical to GDPR and is explicitly extraterritorial in application. GDPR ADVISOR, https://uk-gdpr.org/territorial-scope. For example, in Article 3, the only difference is that the phrase "union" swapped for "United Kingdom." Thus, if a legal hold on a natural person in an EU country would constitute data processing under GDPR, then a legal hold on a natural person in the UK would also constitute data processing under the UK GDPR.

90. DLA Piper, *Law: United Kingdom*, DATA PROTECTION LAWS OF THE WORLD, https://www.dlapiperdataprotection.com/index.html?t=law&c=GB (last modified Jan. 27, 2021).

91. Federal Act of 19 June 1992 on Data Protection (FADP), SR 235.1; Ordinance of 14 June 1993 to the Federal Act on Data Protection (OFADP), SR 235.11; Ordinance of 28 Sept. 2007 on Data Protection Certification (DCPO), SR 235.13. A new update to the FADP was approved in September 2020 and is expected to come into effect on Sept. 1, 2023.

92. Federal Act on Data Protection (FADP), art. 3(e), unofficial English translation available at https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en.

similar to the GDPR definition of processing,[93] and it is therefore likely that implementing a U.S. legal hold involving the personal information collected from individuals in Switzerland would be considered processing under the FADP and thus require the controller to meet the requirements of the FADP. The Swiss FADP's primary provisions are similar to the GDPR, with only minor conceptual differences.[94]

2. Latin America

Brazil: Brazil's General Data Protection Law, Law 13.709 of 2018 (*Lei Geral de Proteção de Dados Pessoais*, or the "LGPD"), came into effect in 2020, with penalty provisions enforced beginning in 2021. The LGPD defines processing as any operation carried out with personal information, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of the information, modification, communication, transfer, dissemination, or extraction.[95] This is similar to the GDPR's definition of processing.[96] Based on these similarities, it is likely that implementing a U.S. legal hold involving the personal information of Brazilian residents would be considered processing under the LGPD, thus requiring a controller to meet the requirements of the LGPD. Also similar to

93. *See* GDPR, *supra* note 1, art.4(2).

94. A revised FADP will go into effect in 2022. *See Data Protected - Switzerland*, LINKLATERS, (last updated June 2022), https://www.linklaters.com/en/insights/data-protected/data-protected—-switzerland.

95. Lei No. 13.709, de 14 de Agosto de 2018, LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD), art. 5 X, *available at* http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

96. *See* GDPR, *supra* note 1, art.4(2).

GDPR, there appear to be risks to relying on consent in Brazil as a lawful basis for preservation under the LGPD.[97]

Argentina: The Argentine Personal Data Protection Law, Act No. 25.326 of 2000 (the "PDPL"), does not define processing, but Section 2 of the Act defines a "data treatment" as any systematic operation or procedure, either electronic or otherwise, which enables the collection, integration, sorting, storage, change, relation, assessment, blocking, destruction, disclosure of data, or transfer to third parties.[98] This is similar to the GDPR's definition of processing.[99] The PDPL has been deemed adequate by the European Commission.[100] Based on these similarities and the adequacy determination, it is likely that implementing a U.S. legal hold involving the personal information of Argentine residents would be considered processing under the PDPL, thus requiring a controller to meet the requirements of the PDPL.

Uruguay: Data protection in Uruguay is governed by the Data Protection Act, Law No. 18.331 of 2008 and Decree No. 414/009 of 2009.[101] In 2012, the European Commission issued an

97. Renato Leite Monteiro, *GDPR matchup: Brazil's General Data Protection Law*, IAPP (Oct. 4, 2018), https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/.

98. Personal Data Protection Act (PDPL) § 2 *(Definitions*), http://www.jus.gob.ar/media/3201023/personal_data_protection_act25326.pdf. *See* Florencia Rosati, *Argentina - Data Protection Overview*, ONETRUST DATA GUIDANCE (NOV. 2022), https://www.dataguidance.com/notes/argentina-data-protection-overview.

99. *See* GDPR, *supra* note 1, art.4(2).

100. *See* DLA Piper, *Law: Argentina,* DATA PROTECTION LAWS OF THE WORLD, https://www.dlapiperdataprotection.com/index.html?t=law&c=AR&c2=FR (last modified Jan 24. 2022).

101. Ley De Proteccion De Datos Personales, Ley No. 18331 (Aug. 11, 2008), *available at* https://www.impo.com.uy/bases/leyes/18331-2008. Reglamen-

adequacy determination allowing for open information transfers between the EU and Uruguay.[102] Given the adequacy determination and the fact that Uruguay's Data Protection Act is similar to the GDPR (although enacted a decade earlier), it is likely that implementing a U.S. legal hold involving the personal information of Uruguay residents would be considered processing, thus requiring a controller to meet the requirements of Uruguay's Data Protection Act.

3. Asia-Pacific

Japan: Japan was one of the first Asian countries to pass a data protection law.[103] Its Act on the Protection of Personal Information ("APPI"), which took effect in 2017, is so similar to the GDPR in terms of fairness, purpose limitation, accuracy, storage limitation, integrity, confidentiality, and accountability that in July 2018, less than two months after the GDPR went into effect, the EU and Japan agreed to declare each other's data protection regimes adequate.[104] The APPI does not expressly define

---

tacion de La Ley 18.331, Decreto No. 414/009 (Aug. 31, 2009), *available at* https://www.impo.com.uy/bases/decretos/414-2009.

102. Commission Implementing Decision of 21 Aug. 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data (2012/484/EU), 2012 O.J. (L 227) 11, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012D0484.

103. *See* Act on the Protection of Personal Information Law No. 57 of 2003, *unofficial translation available at* https://www.japaneselawtranslation.go.jp/en/laws/view/2781. Also, in 2016, the government agency now known as the Personal Information Protection Commission ("PPC"), was established.

104. A tentative translation of Japan's Amended Act of Protection of Personal Information (APPI, version 2, Dec 2016) is available at https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf. The EU and Japan's "reciprocal adequacy" established the largest area of safe data flow in the world.

"processing," but given the overall similarities between the GDPR and the APPI, it is likely that implementing preservation steps as to personal information in compliance with U.S. law would be considered processing under the APPI.[105]

China: China has various laws that limit the collection and use of personal information, such as the Cyber Security Law of the People's Republic of China, which limits the collection and use of personal information (defined as information that alone or in combination with other information could be used to identify a person), establishes information security and data localization requirements, and provides for fines of up to RMB 1 million (roughly $150,000) for violations.[106]

China's Personal Information Security Specification ("PI Specification"), which took effect on October 1, 2020, also regulates the collection and use of personal information. It expands the definition of personal information to include information reflecting an individual's activities such as location data and online browsing history, and it adds the concept of Sensitive Personal Information, which includes a person's ID card number, bank account number, and the personal information of minors.[107] While there are various similarities between the current

---

105. The current version of the APPI distinguishes between public and private entities and applies to "business operators." However, recent revisions in April 2022 have brought other relevant laws in line with some APPI definitions: notably the definition of personally identifiable information (PII), and applications to public entities such that hospitals, other medical research institutions, and some public organizations that regularly use PII will fall under the APPI.

106. *See* Rogier Creemers, et al., *Translation: Cybersecurity Law of the People's Republic of China [Effective June 1, 2017]*, NEW AMERICA (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

107. National Standard of the People's Republic of China, Information security technology—Personal Information (PI) security specification, GB/T

laws and the GDPR, it is not clear whether implementing preservation steps as to personal information in compliance with U.S. law would be considered processing.

China is considering revisions to its data protection laws. On October 21, 2020, the first version of the draft Personal Information Protection Law ("Draft PIPL") was introduced. It would serve as China's first comprehensive data protection law and is intended to have a similar effect as the EU GDPR. It may go beyond the PI Specification. A second version of the Draft PIPL was issued on April 29, 2021.[108]

The Draft PIPL defines "personal information handling" to include the collection, storage, use, processing, transmission, provision, and publishing of personal information.[109] Further, the Draft PIPL more closely mirrors the GDPR, including, for example, its consent principles.[110] Given the similarities to the GDPR, it is likely that implementing a U.S. legal hold involving the personal information of Chinese residents would be considered processing under the Draft PIPL, but this draft has not yet been finalized and promulgated.[111]

35273-2020 (implementation date Oct. 1, 2020), English translation available at https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf. SPI is defined at § 3.2.

108. *See* Hunton Andrews Kurth, *China Issues Second Version of the Draft Personal Information Protection Law for Public Comments*, NAT'L L. REV. (May 4, 2021), https://www.natlawreview.com/article/china-issues-second-version-draft-personal-information-protection-law-public.

109. Creemers, et al., *supra* note 106.

110. Ken Dai & Jet Deng, *China's GDPR is Coming: Are You Ready?*, DENTONS (Mar. 11, 2021), https://www.dentons.com/en/insights/articles/2021/march/11/chinas-gdpr-is-coming-are-you-ready.

111. Gil Zhang & Kate Yin, *A look at China's draft of Personal Information Protection Law*, IAPP (Oct. 26, 2020), https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/.

Singapore: Singapore's Personal Data Protection Act ("PDPA") has a broad definition of processing similar to the GDPR that includes "recording" or "holding" data.[112] It is therefore likely that implementing preservation steps in compliance with United States law would be considered processing in Singapore and regulated by the PDPA.[113]

The PDPA has several differences from the GDPR. Consent under the PDPA is treated more broadly than under the GDPR and includes a number of exceptions allowing implied or "deemed" consent.[114] Similarly, there is no explicit requirement for data minimization. The purpose requirement for processing information only requires a showing of reasonability.[115] Lastly, there is no extra level of protection for sensitive personal information such as race, ethnicity, or religion.[116]

---

112. Personal Data Protection Act (PDPA) 2012 § 2, Law No. 26 of 2012, https://sso.agc.gov.sg/Act/PDPA2012.

113. *Id*.

114. Personal Data Protection Commission (PDPC) Singapore, Advisory Guidelines on Key Concepts in the Personal Data Protection Act (revised May 17, 2022), *available at* https://www.pdpc.gov.sg/guidelines-and-consultation/2020/03/advisory-guidelines-on-key-concepts-in-the-personal-data-protection-act; *see also* PDPA, *supra* note 112, § 15.

115. PDPA, *supra* note 112, § 3.

116. *See, for example,* Advisory Guidelines on Key Concepts in the Personal Data Protection Act, *supra* note 114.

III. PRACTICE POINTS

The following eight practice points are offered to help organizations and counsel navigate international legal holds that may potentially conflict with international data protection laws. Given that many international data protection laws appear to be based in whole or part on the GDPR and that the U.S. arguably has the most significant preservation requirements, the practice points are focused solely on the interplay between U.S. legal holds and the GDPR. The broader goal remains, however, to provide a framework for counsel implementing international legal holds wherever they may arise and that may conflict with international data protection laws, including but not limited to the GDPR.

1. Determine Whether the Preservation of Personal Data Is Necessary, and Then Determine Whether a Data Protection Law Applies

Once the duty to preserve has been triggered, an organization should promptly identify sources of discoverable information that may need to be preserved. Since most data protection laws focus on personal information, the first step is to analyze whether personal information must be preserved.

As discussed in Section II.B, personal information under many data protection laws is broadly defined. Thus, personal information is almost always contained within the sources of information to be preserved. There are certain data sources, however, that are not likely to contain personal information, including software, technical drawings, measuring or construction data, controller's financial data, marketing material, or public communications material. If preservation in a matter is limited to these types of information, it may be possible that

preservation would not give rise to data protection obligations.[117] This would only be true, however, if there were no personal information at all included in the materials.

If personal information must be preserved, the next step is to assess whether another nation's data protection law applies to the data to be preserved. As discussed in Section II.B, the GDPR protects the personal information of natural persons who are in the EU and looks to controllers and processors to enforce its requirements. Controllers and processors are subject to the GDPR's requirements if they do business in the EU or they are based outside the EU but offer goods and services to, or monitor, individuals in the EU. Thus, to determine whether the GDPR applies to a U.S. legal hold, organizations must first identify the controller of the personal information to be preserved and determine whether the controller is subject to the GDPR.

2. Apply the Data Protection Law's Guiding Principles for Processing Personal Information to Every Preservation Step or Process

As discussed in Section II.C.2, Article 5 of the GDPR sets forth guiding principles that govern the processing of personal information. The GDPR's principles include the requirements of:

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation

117. There may be other local laws or regulations, as well as contractual obligations, that impact decisions on processing and subsequent data transfer, including trade secret laws. Thus, counsel should consider consulting local counsel.

- Integrity and Confidentiality; and
- Accountability.

These principles contain objectives for the design of data processing systems and the implementation of data processing operations.[118] Under the GDPR, these principles are a necessary element of each and every step in the scoping, implementation, maintenance, and eventual release of a legal hold. Thus, when implementing a legal hold, counsel should consider how the data protection principles will impact each step of the preservation process.

As noted in the introduction, this *Commentary* does not address cross-border data transfers. Nevertheless, the GDPR imposes additional requirements when transferring data outside of the EU/EEA or to jurisdictions that lack an adequacy determination.[119] Thus, under the GDPR, data should ideally be preserved in its native repository (preserved "in place") or copied and retained within jurisdictions deemed to have adequate privacy protections, and practitioners should exercise caution when transferring data across borders.[120]

3. Document the Lawful Basis for Preservation and Preservation Steps Taken Thereafter

118. Roßnagel, in: SIMITIS, ET AL., *supra* note 33, Art. 5, Rz. 21.

119. *See* GDPR, *supra* note 1, Chapter 5, arts. 44–50.

120. *See* The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)* (Jan. 2017), available at https://thesedonaconference.org/publication/International_Litigation_Principles [hereinafter *International Litigation Principles*]. (Principle 5: "A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.").

A key GDPR principle that all controllers must adhere to when taking preservation steps is the accountability principle. GDPR Article 5(2) states:

> The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').[121]

Thus, to comply with the principle of accountability under the GDPR, counsel should document each step in the preservation process.[122] Documentation created and maintained by the controller or its designee should address:

1. What information is subject to preservation;
2. The purpose for preservation;
3. The length of preservation;[123]
4. The nature of the preservation steps taken;
5. The measures taken to communicate preservation decisions to the affected data subjects;[124]

---

121. GDPR, *supra* note 1, Art. 5(2).

122. *See* European Data Protection Supervisor, *Accountability*, https://edps.europa.eu/data-protection/our-work/subjects/accountability_en (last visited May 19, 2023).

123. Under Article 13 of the GDPR, the length of preservation is the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

124. In some cases, it may be impractical, or even detrimental to an investigation, to provide advance or contemporaneous notice to a data subject. One key example discussed in Practice Point 6, *infra* note 144, is a situation where the data subject may be the subject of the investigation, and there is reasonable grounds to fear that the subject might destroy relevant information if informed of the investigation. This is often called a silent hold, which is allowed under the GDPR in exceptional circumstances. In situations where the company or counsel feel that a silent hold is required, counsel should consider discussing the situation with the appropriate data authority in advance or shortly after the hold is implemented.

6. The measures taken to protect the information from unlawful use or disclosure, including security measures;[125] and

7. Communications with data protection officers or other authorities about the preservation efforts.[126]

The documentation can be maintained in a variety of formats but is most often kept in spreadsheets or in software designed for that purpose.

The controller should initially document the circumstances establishing that the duty to preserve has been triggered. Documentation should begin as soon as the preservation obligation has been triggered. The lawful basis for preservation, to the extent it differs from the triggering event, should also be recorded.[127]

The principle of accountability continues to apply after a lawful basis has been established.[128] This principle requires

---

125. Data security is always a consideration when collecting ESI for a legal hold, particularly if that data is being copied and removed from its protected, secure native environment. The Sedona Conference Working Group 11 has published multiple papers providing guidance on this topic, which are available at https://thesedonaconference.org/publications under the section labeled "Data Security and Privacy."

126. *See, e.g.*, EUROPEAN DATA PROTECTION SUPERVISOR, LEADING BY EXAMPLE: EDPS 2015-2019, *available at* https://op.europa.eu/webpub/edps/edps-2015-2019-report/en/ (last visited May 19, 2023).

127. In documenting the lawful basis for preservation, counsel should be careful about including information that may be otherwise protected by the attorney-client privilege under U.S. law. *See* Practice Point 6, *infra*, at notes 151-152. *See also Sedona Commentary on Legal Holds, Second Edition, supra* note 4.

128. *See, e.g.*, UK GUIDE TO GDPR, *supra* note 83, *Accountability and governance*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/ (last visited May 19, 2023).

controllers to continue to document their decision-making in connection with each step of the preservation process.[129] In each case, the documentation should describe the preservation alternatives considered and the rationale for selecting one route over another.[130]

Documentation provides an effective means to defend the organization's actions should they be questioned at a later time. Further, documentation is necessary not only for potential review by the data protection authority but also to respond to data subject inquiries about whether personal information is being processed.[131] As noted earlier, counsel should consider using technology to be able to track and respond to requests in a timely manner.

4. Take Steps to Minimize the Scope of Preserved Information

Minimization is one of the GDPR's leading principles and allows information to be processed only if it is "adequate, relevant," and specifically limited to achieve the intended purpose.[132] For example, instead of reflexively placing a custodian on legal hold because of his or her title or department, counsel may—through interviewing, reviewing organizational charts, or taking other steps—consider whether the individual's information really has significance regarding the matter before placing the custodian on legal hold. Counsel may also prioritize certain custodians' sources or limit the particular sources that need

---

129. *See generally* Robert Healey, *GDPR and the Accountability Principle*, FORMITI (Aug. 10, 2022), https://formiti.com/gdpr-and-the-accountability-principle/.

130. *Id*.

131. *See* GDPR, *supra* note 1, art. 15 (*Right of access by the data subject*).

132. *See* GDPR, *supra* note 1, art. 5(1)(c): personal information shall be: "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')."

to be preserved rather than automatically deciding that all of a custodian's sources should be preserved. Similarly, some litigants employ "preservation in place" strategies within repositories that support the capabilities to do so, such as suspending the auto-delete function in an email system for identified custodians, or keeping a copy of subsequently modified or deleted content within the repository itself.[133] Although this last step still constitutes processing within the meaning of the GDPR, it at least reduces the overall exposure of the information to other parties. Another approach is to remove custodians' rights to alter or delete documents in their possession or control. And yet a third approach is to rely on custodians to take action to preserve information in their possession, custody, or control.[134]

---

133. Some may argue that suspending the auto-delete function in order to achieve preservation may be in conflict with the minimization principle. Wherever possible, auto-delete functions should be suspended specifically for the relevant information subject to litigation hold, such as individual mailboxes. Custodians would still have the ability to manually manage and delete content unrelated to the legal hold, thus ensuring minimization. Furthermore, some systems can prevent the deletion of data via a legal hold function (which overrides both retention rules and user deletion actions); while still others implement an affirmative preservation in place and prohibit alteration or deletion of a particular document. With auto-delete, for example, a custodian could still delete the email. *See* GDPR, *supra* note 1, art. 17 (1)(a), Recital 65: allowing the further retention of the personal data that is no longer necessary in relation to the original purposes but necessary for legal defense.

134. Various authorities have confirmed that parties can rely on the good-faith actions of their employees in the preservation process so long as the process is properly supervised by case counsel. *See* Radiologix, Inc. v. Radiology & Nuclear Med., LLC, No. 15-4927-DDC-KGS, 2019 WL 354972, at *11 (D. Kan. Jan. 29, 2019) (producing party's reliance on custodians for identification and collection along with counsel's supervision of the process was appropriate and court "declines to conclude—in hindsight—that plaintiffs should have used different collection or searching methods to identify and produce relevant documents before trial"); *see also* New Mexico Oncology &

Although these last steps still constitute processing within the meaning of the GDPR, they at least delay the exposure of the information to other persons unless and until it is needed, and in some cases it may become unnecessary to collect the data if it turns out to be irrelevant or otherwise immaterial.

Some U.S. litigants, due to cost, burden, proportionality, and business interruption reasons, already take minimization concepts into account when preserving information under U.S. law.[135] Litigants who are not already using these more deliberative preservation strategies in the U.S. generally should consider employing them when preserving personal information that is subject to the GDPR to comply with the GDPR's minimization principle.[136] Furthermore, under minimization principles, counsel should consider reserving collection of or copying information for preservation purposes only when absolutely required to do so to ensure adequate protection of discoverable

---

Hematology Consultants, Ltd. v. Presbyterian Healthcare Servs., No. 1:12-cv-00526 MV/GBW, 2017 WL 3535293 (D.N.M. Aug. 16, 2017) (litigation hold effectuated through self-preservation not inadequate where custodians "were directed to retain documents and data 'that mention or discuss or relate to any of' an exhaustive list of subjects" and were "also directed that if 'you are unsure about the relevance of a document, be cautious and preserve it'"); *Sedona Commentary on Legal Holds, Second Edition*, *supra* note 4, at 408. ("[I]n most cases, a careful combination of notification as described above, collection, and individual action should enable parties to rely on the good-faith actions of their employees").

135. *See Sedona Commentary on Legal Holds, Second Edition*, *supra* note 4, at 389 (Guideline 7: "Factors that may be considered in determining the scope of information that should be preserved include the nature of the issues raised in the matter, the accessibility of the information, the probative value of the information, and the relative burdens and costs of the preservation effort.").

136. *See* GDPR, *supra* note 1, art. 5(2): "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

data—for example, where the information is in the hands of someone likely to destroy relevant information, or where the information is ephemeral in nature and likely to be otherwise lost. In such cases, the reason for preservation should be documented thoroughly and be based on principles of minimization.

5. Consider Involving Data Protection Officers, Supervisory Authorities, or Work Councils

Under the GDPR, data protection officers are appointed by controllers to advise on and monitor GDPR compliance. A data protection officer may be either an employee or an external service provider such as external legal counsel. The data protection officer holds a somewhat independent position and acts as the contact between controller and the supervisory authority.[137]

The GDPR requires controllers to involve data protection officers in a timely manner when issues arise relating to the protection of personal information, including issues relating to a controller's legal hold process developed to comply with U.S. law.[138] Practically speaking, however, involving data protection officers in the legal hold process would only come into play in limited circumstances. Controllers are more likely to involve data protection officers with nonroutine preservation issues to obtain guidance and insight into formal or informal opinions of supervisory authorities[139] and/or obtain helpful indications on the interpretation of local laws. Controllers may also decide to involve a data protection officer in some matters because it may

137. *Id*. at art. 39, Recital 97 (*Data protection officer*).

138. *Id*. at art. 38.

139. Data protection authorities frequently issue advice or practical tips on their websites or publish instructive articles in law journals on their interpretation of the law.

reflect well on the organization's commitment to protecting the rights of data subjects.[140]

Because some jurisdictions in the EU have strict labor laws and rules on employee representation, many organizations have agreements that detail the legal hold process in connection with employee rights.[141] Where appropriate, counsel should consult local counsel regarding the existence of local agreements prior to taking preservation steps in connection with a matter. Even in the absence of such an agreement, counsel should consider seeking guidance from the local works council[142] or other employee representatives before a legal hold is issued. This demonstrates transparency and also helps ensure a consistent and reasoned response from the organization should the employee reach out directly to the works council or employee representatives for guidance.

Early notice also enables the works councils to exercise their rights in an informed manner, which further protects the data subject's rights.[143] In some jurisdictions, employees have the

---

140. *International Litigation Principles*, *supra* note 120.

141. Under German law, a company can negotiate an agreement with the collective works council laying out in great detail specific processes, including details on issuance of a legal hold.

142. A works council is an institutionalized employee representation body in companies and corporate groups that represents the co-determination body under works constitution law. In Germany, by law, the works council resulting from a works council election is the representative of the workforce. *See* Betriebsverfassungsgesetz [BetrVG] [Works Constitution Act 1972], § 1. Counsel should keep in mind that various forms of employee representations exist in different countries.

143. GDPR, *supra* note 1, Recital 60 (*Information obligation*) highlights that the principle of *fairness* requires controllers to provide the data subject with any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal information is processed.

right to ask for the presence of a works council member during legal interviews, such as during preservation interviews. This is particularly important if the individual could be subject to discipline in connection with the matter.

6. Communicate Clearly with Data Subjects, Advising What Materials the Organization is Preserving, and What Steps Will be Taken as to Personal Information

Giving notice to affected individuals that their information is being preserved pursuant to a pending U.S. legal matter is a key requirement of the GDPR. While there are some noteworthy exceptions to the duty to inform,[144] under the GDPR, data subjects must, in general, receive notice that personal information is being processed, the reasons for preservation (processing), an explanation of their rights, and a means to exercise their rights.[145]

More specifically, GDPR Article 13(1) requires that the following information be provided where personal information is collected from the data subject:

144. In exceptional cases, the duty to inform does not apply. Such cases include situations where the notice about the intended further processing would interfere with the establishment, exercise, or defense of legal claims and where the controller's interest in not providing the information outweighs the data subject's interest. *See, e.g.*, Germany's Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], June 30, 2017, § 32. If the notification is not provided due to such interference, the controller shall periodically re-evaluate whether the original or new cause for withholding the information continues to exist. When the controller determines that providing notice will no longer result in such interference, the controller should then provide proper, timely notice to the data subject.

145. GDPR, *supra* note 1, art. 13(1).

> (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
>
> (b) the contact details of the data protection officer, where applicable;
>
> (c) the purposes of the processing for which the personal information is intended as well as the legal basis for the processing;
>
> (d) the legitimate interests pursued by the controller or by a third party;
>
> (e) the recipients or categories of recipients of the personal information, if any; and
>
> (f) where applicable, the fact that the controller intends to transfer personal information to a third country or international organisation.

The principle of *transparency* requires that such information be easy to understand.[146]

Controllers likely already have in place general information regarding their processing practices, such as a privacy notice for employees.[147] These general notices may only address processing that occurs in the regular course of business in an employment context and not fully describe all aspects of processing needed for preservation in a U.S. legal matter. Counsel should consider issuing matter-specific notices, written in clear and simple language, to communicate with data subjects about

146. *See supra* Section II.C.2.

147. Agreements between a controller and local unions or works councils may contain provisions outlining systems and procedures for issuing legal holds to employees. *See also supra* Section III.5, nn. 141–43.

preservation. An example of a notice that incorporates the GDPR's requirements is attached as Appendix A.

Many organizations handle the notification described above by addressing it in written legal hold notices. Under these circumstances, the legal hold notice should include information about the privacy rights of the data subjects and use of their personal information.[148] Referring to FAQ documents or other

148. Counsel should consider referencing GDPR Article 5 principles for the protection of personal information. Counsel should also recognize the conflict between U.S. preservation law and EU law on the required preservation of relevant personal information. Pursuant to Rule 34 of the Federal Rules of Civil Procedure, some U.S. courts have required organizations to preserve potentially relevant personal webmail of employees and/or the potentially relevant text messages stored on personal mobile devices on the theory that corporations are deemed to have control over their employees work-related documents, whether located at the office or at home. Paisley Park Enters., Inc. v. Boxill, 330 F.R.D. 226 (D. Minn. 2019) (finding defendants failed to preserve relevant text messages from executives' personal devices used for company business); Fluke Elecs. Corp. v. CorDEX Instruments, Inc., No. C12-2082JLR, 2013 WL 566949, at*13 (W.D. Wash. Feb. 13, 2013) (noting that litigants owe a duty to preserve what they know or reasonably should know will be relevant evidence, including ESI from personal and home computers and other devices); Helmert v. Butterball, LLC, No. 4:08CV00342 JHL, 2010 WL 2179180, at *9 (E.D. Ark. May 27, 2010) (ordering corporation to produce email from personal email accounts from upper management employees over the corporation's objection that it did not have access to the employees' accounts). German civil law states that upon termination of the employment relationship, an employee must return all business documents that have been made available by the employer or the employer's representative (so called "duty to return," *see* BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE], § 667, alt. 1, as well as those which the employee has obtained during the employment relationship, *e.g.*, through correspondence with a third party, *id.* § 667, alt. 2; files, other documents, and files that the employee has prepared himself in connection with his work, as well as copies of such documents, must also be returned (*See* Bundesarbeitsgericht [BAG] [Federal Labor Court], Dec. 14, 2011, NZA 2012, 501; Christoph Bergwitz, *Zurückbehalten von Geschäftsunterlagen*, NZA 2018, 333). However, this duty to return does

internal reference materials relating to legal holds that help a custodian better understand what is being asked of them when responding to a legal hold notice can also demonstrate transparency and consistency. In addition to general FAQs addressing legal holds, a controller may wish to have country- or jurisdiction-specific addendums that include appropriate legal notices or statements informing employees of their privacy rights and available resources.

One approach may be to keep the notice relatively short but to include links to FAQs and, if appropriate, to include links to country-specific standard addendums or FAQs.

Notice should be provided as quickly as possible.[149] Under the GDPR, notice should be provided upon or before the commencement of any preservation activities.[150]

In fulfilling preservation obligations, counsel should be aware that not all jurisdictions recognize that legal hold notices or related communications are protected by the attorney-client privilege or work-product doctrine. U.S. courts typically find that legal hold notices are protected by the attorney-client privilege and the work-product doctrine.[151] In contrast, jurisdictions outside the U.S. that recognize similar concepts of attorney-

---

not give the employer the right to demand surrender of the employee's entire private device, which he may have used to create such communication or files.

149. *See also* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, 17 SEDONA CONF. J. 397, 409 (2016) (Principle 5: "A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.").

150. GDPR, *supra* note 1, art.13(1).

151. Typically this protection is based on the attorney-client privilege and the work-product doctrine. *See* Gibson v. Ford Motor Co., 510 F. Supp. 2d 1116, 1123–24 (N.D. Ga. 2007).

client privileged communications or attorney work product do not typically consider legal hold notices or preservation steps to be privileged except when external counsel are involved.[152] Organizations should consider whether outside counsel should draft the legal hold notice and be consulted on preservation steps.

7. Make Sure Legal Hold Notices are Translated in Accordance with Local Law

Local laws may require that "business communications" or "employee communications" be translated.[153] It is not always clear whether a legal hold notice constitutes a "business communication" requiring translation. The conservative approach is to treat a legal hold notice as a business communication and incorporate translations when appropriate.[154]

Translation of a legal notice into the native language of the recipient is consistent with the GDPR principle of transparency.

---

152. For example, Japan does not currently protect "communications between a corporation and non-*bengoshi* in-house lawyers [i.e., in-house counsel]." Masamichi Yamamoto, *How Can Japanese Corporations Protect Confidential Information in U.S. Courts?*, 40 VAND. J. TRANSNAT'L L.503, 515 (2007).

153. Providing hold instructions in a native or local language can also foster better understanding and demonstrate good faith in addressing preservation obligations. For example, in *E.I. du Pont de Nemours & Co. v. Kolon Industries*, a dispute arose after non-English speaking employees were found to have spoliated relevant information. The court ultimately imposed sanctions, finding that the company had failed to affirmatively monitor compliance by non-English speakers with a legal hold notice issued in English. 803 F. Supp. 2d 469, 479 (E.D. Va. 2011). The legal hold notice was written in English and distributed mostly to non-English speaking employees of a South Korean company (in addition to its United States subsidiary). Ultimately, the Court imposed sanctions in the form of attorneys' fees, expenses, costs, and an adverse inference instruction. *Id*. at 510.

154. Belgium, France, Québec, Spain, Mongolia, Kuwait, Saudi Arabia, Turkey, Slovakia, Poland, and Venezuela are a few jurisdictions with local laws governing employee communications.

Moreover, many Civil Code jurisdictions require that business documents be translated into an individual's primary language.[155] Belgian law, for example, requires that business documents between employer and employees be provided in Dutch, French, or German, depending on the individual's primary language.[156] Likewise, France requires that business documents between employer and employee be in French.[157] While Civil Code jurisdictions tend to have laws requiring translation of certain business and/or employee communications into native languages, common law jurisdictions generally allow business communications to be in English and do not have strict statutory translation requirements. Counsel should consider consulting with local counsel regarding appropriate interpretation of the local laws and their application to legal hold notices.

Even when not required, providing legal hold notices in the recipient's native language can help ensure that recipients understand the notice. It is also important to consult and follow the organization's internal policies on translation of business communications.

8. Reevaluate and Release Legal Holds and Dispose of Information When No Longer Needed

As a matter progresses, the scope of a legal hold may change, expanding in some cases and narrowing in others. When it does, organizations subject to a U.S. legal hold are expected to

---

155. UK GUIDE TO GDPR, *supra* note 83, *How should we draft our privacy information?*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/how-should-we-draft-our-privacy-information/ (last visited May 19, 2023).

156. Decree of the Vlaamse Gemeenschap [on the use of languages] of July 19, 1973, BELGISCH STAATSBLAD [Official Gazette of Belgium], Sept. 6, 1973, 10089.

157. *See* CODE DU TRAVAIL [C. TRAV.] [LABOR CODE] art. L.1321-6.

reevaluate the scope of the hold notice and amend it as necessary.[158] This is particularly important for legal holds involving personal information subject to the data protection law. For example, failing to address changes to the scope of the legal hold could violate three key GDPR processing principles: "purpose limitation," "data minimisation," and "storage limitation."[159]

Under the GDPR, the purpose limitation requires that personal information be collected only "for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[160] Personal information that has been placed on legal hold and preserved cannot be processed for any other purpose. If the scope of the matter changes, the controller must evaluate whether the original purpose still exists or if other matters or issues can support the original purpose. If the original purpose no longer exists, or the matter has terminated, then the GDPR requires that the legal hold be terminated and the personal information released from the hold.[161] Changes in scope may require the controller to revise the notice.

---

158. Guideline 8(f) of the Legal Hold Guidelines recommends that legal hold notices be "periodically reviewed and amended when necessary." *Sedona Commentary on Legal Holds, Second Edition*, *supra* note 4, at 399.

159. GDPR, *supra* note 1, art. 5(1)(b), (c), and (e).

160. *Id.* at art. 5(1)(b).

161. In 2019, the Berlin data protection commissioner had issued a fine notice of 14.5 million Euros against Berlin's largest private landlord. *See* https://openjur.de/u/2331402.html. This was the highest fine to date in Germany based on the GDPR. Deutsche Wohnen was fined because personal data of former tenants, such as social and health insurance data, employment contracts, or information about their financial circumstances, could still be viewed and processed via the company's archive, and the archive had no technical functionality to delete data. The authority had already drawn the company's attention to the irregularities in 2017 and demanded a remedy. The Berlin Regional Court declared the decision of the Berlin data protection commissioner to be invalid because it lacked details of specific acts. Subsequently, the public prosecutor's office, in agreement with the state data

The principle of data minimization under the GDPR also limits the use of personal information to "what is necessary in relation to the purposes for which they are processed."[162] This principle applies to information that was once subject to the duty to preserve but is determined later to be not discoverable and thus no longer "necessary" for preservation purposes. Under these circumstances, organizations should release the applicable custodians and data sources from a legal hold and, if otherwise appropriate, dispose of personal information. This can include information that was culled based on search criteria that have not been challenged or have been agreed to by opposing counsel, and no future challenge is anticipated.

Under the principle of storage limitation, personal information must not be retained in a form that permits the identification of a data subject for any length of time that is "longer than necessary for the purposes for which the personal data are processed."[163] Accordingly, personal information that is no longer required to be preserved under a U.S. legal hold and is not otherwise needed by the organization must be released and/or any collected information destroyed as soon as possible once the information is no longer needed for the matter.[164]

---

protection commissioner, filed an appeal before the Kammergericht, which in late 2021 turned to the European Court of Justice for guidance. Regardless of the outcome of the proceedings, it is clear that data protection authorities are prepared to impose heavy fines and are not afraid to exhaust legal remedies.

162. GDPR, *supra* note 1, at art. 5(1)(c).

163. *Id*. at art. 5(1)(e).

164. *See Sedona Commentary on Legal Holds, Second Edition*, *supra* note 4, at 408–09.

IV. CONCLUSION

Controllers or processors doing business in the EU or who offer goods or services to EU residents or monitor their behavior within the EU, and who are required to implement preservation steps as to data subjects' personal information pursuant to a U.S. legal hold, must comply with the requirements of the GDPR. The *Commentary* provides eight practice points above to help counsel comply with the GDPR under these circumstances. The practice points should also provide a useful framework for counsel implementing international legal holds in other jurisdictions beyond the U.S. and that may have conflicting international data protection laws beyond the GDPR.

APPENDIX A

Sample Notice Incorporating GDPR Requirements

Dear [recipient],

[Company name] is involved in a matter [provide high level detail regarding investigation, lawsuit, etc.] pending in the United States District Court for the [detail court information].

By law, the company is required to preserve information that may be relevant and ensure that such relevant information is not modified or destroyed. You are receiving this notice because you may have relevant information regarding this matter. Information that must be preserved includes email and other types of electronic communications, documents (paper or electronic), or other electronically stored information and/or paper documents. Relevant information may also include personal information that may identify you, such as your name, email address, telephone number, or other personal identifiers.

The company has a legitimate interest in preserving your personal information to comply with its legal obligations in connection with the matter. The legal basis for processing your personal information is GDPR Art. 6 (I) (f). The personal information will be preserved until the matter is completely resolved and the company no longer has a legal obligation to preserve it.

To preserve the information, the company may take some or all of the following steps:

1. Search for information that may be relevant to the matter. The search may include the following steps [insert information about the search and scope of the data investigation]. Additional steps may be taken should the company's understanding regarding the scope of the matter change in the future.
2. Make copies of any of the personal information described above.

3. Review information to determine whether it is relevant to the matter.
4. Create information about the personal information for analysis purposes and to help fulfill the company's legal responsibilities.
5. Share information with other company employees participating in the matter or with legal counsel or others hired with respect to the matter.

Depending on how the matter progresses and the company's legal responsibilities, the company may ultimately be required to transfer some of the preserved personal information to another country, including countries with no adequacy decision by the European Commission, for review by legal authorities or other counsel involved in the matter.

With respect to the processing of your personal information in this matter and to the extent granted by GDPR, you have the following rights:

1. The right to request information about, to access, or to receive copies of your personal information in a form readable by you;
2. The right to ask to correct personal information about you that is being preserved (which may be granted or not depending on the company's legal obligations);
3. The right to ask the company to delete certain personal information (which may be granted or not depending on the company's legal obligations);
4. The right to ask for restriction of processing;
5. The right to object to the preservation of personal information about you (which may be granted or not depending on the company's legal obligations);

6. The right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before withdrawal of consent; and
7. The right to file a complaint about preservation of your personal information with the following supervisory authority: [name and contact information].

If you have any questions regarding this notice or wish to object to the preservation of your personal information, please contact the responsible controller at:

> [name of controller and contact person along with email, address and phone information.]

You may also contact the data protection officer at:

> [name of data protection officer and contact information, with explanation of who and why to contact either.]

The company will keep you advised regarding the progress of the matter and the preservation of your personal information. The company will also notify you when the matter is resolved and the company's obligation to preserve personal information has ended.

Thank you for your cooperation and understanding. If you have questions or concerns about this letter, please feel free to contact:

[Contact information of the writer or other suitable person]
Signed
Title

THE SEDONA CONFERENCE FRAMEWORK FOR ANALYSIS FOR THE EFFICIENT RESOLUTION OF DISPUTES BEFORE THE FORTHCOMING EUROPEAN UNIFIED PATENT COURT

A Project of The Sedona Conference Working Group on Patent Litigation Best Practices (WG10)

Author:

The Sedona Conference

Editor-in-Chief:

Matthew Powers

Managing Editors:

Jim W. Ko
David Lumia
Casey Mangan

Chapter Editors:

Philipp Widera
Tobias Wuttke

Contributing Editors:

Rainer Beetz
Mikkel Bender
Koen Bijvank
Benjamin Grzimek
Aloys Hüttermann
Vittorio Cerulli Irelli
Martin Levinsohn
Amandine Métier
Tilman Müller-Stoy
Jane Mutimear
Michael Rüberg
Massimo Sterpi

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The

Sedona Conference's Working Group 10. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any organizations to which they may belong, nor do they necessarily represent official positions of The Sedona Conference.

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, click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> The Sedona Conference, *Framework for Analysis for the Efficient Resolution of Disputes before the Forthcoming European Unified Patent Court*, 24 SEDONA CONF. J. 219 (2023).

PREFACE

Welcome to the May 2023 Final, Post-Public-Comment Version of *The Sedona Conference Framework for Analysis for the Efficient Resolution of Disputes before the Forthcoming European Unified Patent Court*, a project of The Sedona Conference Working Group on Patent Litigation Best Practices (WG10). 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, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG10 is "[T]o develop best practices and recommendations for patent litigation case management. The Working Group is composed of members of the federal trial and appellate court benches, litigators who primarily represent patentees, and those who primarily represent accused infringers in federal court, the Patent Office, and the ITC."

The *Framework for Analysis for the Efficient Resolution of Disputes before the Forthcoming European Unified Patent Court* drafting team was launched in 2019 and is led by editors Philipp Widera and Tobias Wuttke. Earlier drafts of this publication were a focus of dialogue at the WG9&10 Joint Annual Meeting in Philadelphia, Pennsylvania, in March 2019; the WG9&10 Joint Annual Meeting, Online, in November 2020; the WG9&10 Joint Annual Meeting, Online, in November 2021; the WG9&10 Joint Annual Meeting in Boston, Massachusetts, in June 2022; and The 2023 Sedona Conference on Global Intellectual Property Litigation, in London, United Kingdom, in January 2023.

This *Framework* represents the collective efforts of many individual contributors. On behalf of The Sedona Conference, I thank in particular Matthew Powers, the Chair Emeritus of WG10, who has served as the Editor-in-Chief of this publication.

I also thank everyone else involved for their time and attention during this extensive drafting and editing process, including: Rainer Beetz, Mikkel Bender, Koen Bijvank, Benjamin Grzimek, Aloys Hüttermann, Vittorio Cerulli Irelli, Martin Levinsohn, Amandine Métier, Tilman Müller-Stoy, Jane Mutimear, Michael Rüberg, Massimo Sterpi, Philipp Widera, and Tobias Wuttke.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG10 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, data security and privacy liability, patent damages and remedies, 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.

Craig W. Weinlein
Executive Director
The Sedona Conference
May 2023

TABLE OF CONTENTS

FOREWORD

Under the impending Unified Patent Court (UPC) system scheduled to begin operations on June 1, 2023, a new patent jurisdiction will arise potentially spanning the whole of the European Union (EU). The advantages are obvious: more cost-efficient litigation with the chance of obtaining an EU-wide injunction. Nevertheless, as with all new laws and regulations (let alone courts), there will be significant uncertainty around the first pending proceedings and how they will be managed by the incipient UPC. To mitigate these uncertainties, judges and lawyers need to consider a whole new set of provisions and rules as well as the existing case law under the different current European patent law regimes to better understand how to interpret the new rules and resolve the disputes in an efficient, fair, and equitable manner.

All stakeholders involved—patentees, defendants, practitioners, and judges—will look for guidance in the relevant provisions, but also in the body of case law formed by national court practice and decisions. There will be a joint struggle to find the best way to litigate incipient European Patents with unitary effect (EP-UEs)—and also those "traditional" European Patents (EP) that have not been opted out of in time—before the new UPC, keeping in mind the potential competition from national courts for shorter, more effective, and cost-efficient national procedures.

WG10's overarching Principle for our efforts in this The Sedona Conference Working Group 10 Framework for Analysis for the Efficient Resolution of Disputes before the Forthcoming European Unified Patent Court is:

Principle No. 1 – The accurate and efficient resolution of EU-wide patent disputes before the UPC will be improved by cross-fertilization of best practices developed in different jurisdictions attempting to solve the same problems, and the newly formed

UPC addressing these disputes will benefit from having a greater understanding of the different approaches taken across Europe.

Working Group 10 will update this *Commentary* to reflect the forthcoming case law as it develops.

Editor-in-Chief
Matthew Powers
Chair Emeritus, Working Group 10 Steering Committee

Chapter Editors
Philipp Widera
Tobias Wuttke

I. INTRODUCTION

Increasingly, multinational corporations with global patent portfolios are seeking to enforce their portfolios on multiple fronts across different patent jurisdictions around the world. In turn, companies that expect to be asked to license such global portfolios are considering strategies to limit their exposure by steering dispute resolution to more favorable venues.

Currently, a patentee[1] cannot enforce its patents in the whole of the European Union (EU) with one action. Even though the term "European Patent" (EP) suggests a European-wide protection, an EP is in fact a bundle of various national patents in territories that are within and outside of the EU. Accordingly, each national court of each member state of the EU can only decide about the infringement or validity of the respective national part of the EP. Even though there are exceptions to this rule, an infringement action must principally be filed in each of the member states of the EU in which the patentee wishes to enforce its rights, irrespective of whether the defendant[2] and the alleged infringing act are identical in each jurisdiction. Most of the largest global patent cases are filed in a handful of venues—with the key EU venues being Germany, the Netherlands, and France—due to perceived advantages (e.g., quality, timing, costs, or available remedies). Nevertheless, the need to file separate patent infringement actions under in part different substantive and procedural law regimes opens the question whether

1. As used herein, the term "patentee" covers all persons or entities having the right to assert a patent before a national court or the UPC (i.e., covering proprietors and exclusive licensees) unless the terms "proprietor" or "(non)exclusive licensee" are expressly used.

2. For the sake of simplicity, this *Framework* consistently uses the term "defendant" to represent both defendants (after infringement action is filed) and alleged infringers (covering potential defendants as well before any infringement action is filed).

individual EU countries will remain attractive venues of choice for the enforcement of global patent disputes for patentees in the future.

The Unified Patent Court (UPC) system will provide a completely new playing field for international patent litigation. The various courts scattered throughout Europe that are about to be established and that jointly form the UPC will decide infringement and validity of European Patents with unitary effect (EP-UEs)[3] and, during a transitional period, all other EPs within its jurisdiction that have not been opted out from the competence of the UPC.

The first attempt to generate a unitary patent system that would span the European Economic Community[4] (EEC) was the 1975 "Convention for the European Patent for the common market," or "(Luxembourg) Community Patent Convention."[5] However, ratification by all then EEC member states could not be achieved. The main reasons for the failure were the anticipated additional costs (due in part to the requirement of full translation of the whole patent document into all languages of the EEC) and the planned dispute resolution process, under which a patent-in-suit might be declared null and void by a single ordinary court and in effect invalidated across the complete territory of the EEC.[6]

---

3. European Patents with Unitary Effect (EP-UEs) are sometimes referred to as Unitary Patents (UPs). This paper, however, consistently uses the acronym EP-UE throughout.

4. The EEC was the predecessor of the European Union, the latter of which was formally established in 1993.

5. *Available at* Https://op.europa.eu/en/publication-detail/-/publication/b884b73a-8a0b-4c34-b1de-f4de8c5fa6df/language-en.

6. Horst-Peter Götting, *Das EU-Einheitspatent - Das Ende einer "unendlichen Geschichte"?*, ZEuP, Vol. 22, No. 2349-370 (2014).

The second attempt was made in 2000 when the European Commission (EU Commission), one of the legislative bodies of the then European Community,[7] published a proposal for a community patent.[8] Essentially, the already existing European Patent Convention (EPC),[9] which was independent from the European Community, was to be connected with the future common European Community patent system. According to this proposal, the European Community was to become a member of the EPC and bring into existence a single European Community patent. Furthermore, the aim was to set up a common court for intellectual property matters consisting of first instance divisions and boards of appeal having sole jurisdiction over patent matters. After this proposal was revised in March 2004,[10] it looked as if it would be ratified and the European Community patent system would launch. However, European Community member states again could not come to agreement on the issues of translation and an effective court system.[11] After further deliberation, the Council of the European Union, one of the legislative bodies of the European Union, agreed in December 2009

7. The European Economic Community was renamed the "European Community" (EC) in 1993.

8. European Commission, Proposal for a Council Regulation on the Community patent, COM(2000) 412 final — 2000/0177(CNS) (Aug. 1, 2000), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0412:FIN:EN:PDF.

9. The European Patent Convention, https://www.epo.org/law-practice/legal-texts/epc.html, [hereinafter *EP Convention*] is a multilateral treaty originally signed by 16 countries in 1973 and instituted the European Patent Organisation. This provided an autonomous legal system according to which European Patents (EPs) are granted.

10. Council of the European Union, Preparation of the Meeting of the Council on 11 March 2004 – Community patent, 7119/04 (Mar. 8, 2004), https://data.consilium.europa.eu/doc/document/ST-7119-2004-INIT/en/pdf.

11. *See* Horst-Peter Götting, *supra* note 6.

on a concept for an EU Patent Regulation[12] that included the creation of a court for EPs and unitary EU Patents (the precursor of the European Patent with unitary effect).

In parallel with this development, the member states of the EPC worked on the European Patent Litigation Agreement aiming at generating a European Patent Court. Even though the EU Commission was in favor of the EU being part of the Litigation Agreement system, the Court of Justice of the European Union found the agreement noncompliant with EU law due to the lack of a mechanism for courts to make referrals to the Court of Justice of the European Union.[13] Additionally, Italy and Spain disagreed with the planned-for language regime of the three official languages of the EPC: German, English, and French.

In order not to stall the development of an EU-wide patent system, the EU Commission and the Council decided in 2011 to make use of the so-called "enhanced cooperation" mechanism.[14] In the sense of a "two-speed Europe," this instrument opened up the possibility of achieving greater integration even if, in the absence of a consensus among all EU member states, only some of them want to participate in a legislative process. Spain and Italy filed a complaint before the Court of Justice of the European Union against the adoption of the "enhanced cooperation" mechanism in relation to patent matters, but the court in April

12. Council of the European Union, Proposal for a Council Regulation on the Community patent – General approach, 16113/09 (Nov. 27, 2009), https://data.consilium.europa.eu/doc/document/ST-16113-2009-ADD-1/en/pdf.

13. Opinion Pursuant to Art. 218(11) Treaty on the Functioning of the European Union (TFEU), Opinion 1/09 (E.C.J. Mar. 8, 2011), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62009CV0001&rid=4.

14. Council of the European Union, Council Decision of 10 March 2011 authorising enhanced cooperation in the area of the creation of unitary patent protection, 2011/167/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011D0167&from=EN.

2013 dismissed their objections as unfounded.[15] In this case, "enhanced cooperation" means that it enters into force only when it has been ratified by thirteen EU member states, including those three with the most valid EPs in the year preceding the year of signature of the Agreement on the Unified Patent Court (UPCA).[16] At that time, those three EU member states were Germany, the United Kingdom, and France.

- This so-called "EU Patent Package" lays the groundwork for the creation of unitary patent protection in the EU, consisting primarily of three pillars: the EU Unitary Patent Regulation,[17] the EU Translation Regulation,[18] and the UPCA.
- As a consequence of the link to the European Patent Convention, the European Patent with unitary effect is a European Patent that has unitary

15. Kingdom of Spain & Italian Republic v. Council of the European Union, Joined Cases C-274/11 and C-295/11 (CJEU Dec. 11, 2012), https://curia.europa.eu/juris/document/document.jsf;jsessionid=F44C99206065F55B9FC1E8C7462FD524?text=&docid=131666&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=718226.

16. Agreement on a Unified Patent Court, EU 2013/C 175/01 [hereinafter *UPC Agreeement*], https://www.unified-patent-court.org/sites/default/files/upc_documents/agreement-on-a-unified-patent-court.pdf.

17. Regulation (EU) No. 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection [hereinafter *Unitary Patent Regulation*], Art. 8(2) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012R1257.

18. Regulation (EU) No. 1260/2012 of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection with regard to the applicable translation arrangements [hereinafter *EU Translation Regulation*], https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012R1260.

effect as from the date of grant of the EP. "Unitary effect" means the EP is in effect in the combined territory of each member state of the EU participating in the UPC system (as if it was one country). It is issued as part of the bundle of national patents as far as the nonparticipating member states of the EU and the remaining non-EU European Patent Convention countries are concerned.[19] For this reason, the EU Unitary Patent Regulation speaks of a "European Patent with unitary effect." The prerequisite for this is that a European Patent has to have been granted according to the rules of the EPC. The EP-UE is thus dependent on the underlying EP.

- The EU Translation Regulation provides that no further translations are required once the patent specification of an EP-UE has been published. Further translations are required only in case of litigation and during the transitional period.
- The newly setup UPC system consists of two instances, namely a court of first instance and a court of appeal. The court of first instance comprises a central division and local and regional divisions.

Further complaints by Spain against the so-called "EU Patent Package" were dismissed by the Court of Justice of the European Union, but a major setback for this project occurred in Germany. In 2017, a constitutional complaint against the nationally necessary approval act for incorporating the UPCA into law

19. For example, the result of an EP-UE could be the grant of a bundle of patents consisting of the following national patents: Norway and Switzerland (both not members of the EU), Spain (currently not participating in the EU Patent Package) and the European Union.

was filed before the German Federal Constitutional Court. In February 2020, the court allowed the complaint and declared the approval act null and void.[20] The approval act would have transferred sovereign rights to the newly created UPC, thus effecting a substantive constitutional amendment. However, according to the court, this lacked the necessary approval of a two-thirds majority of all members of the *Bundestag* (Parliament) and the *Bundesrat* (Federal Council). The unanimous resolution of the Parliament, at which only 35 parliamentarians were present, was therefore not sufficient. Accordingly, Germany (as one of the necessary signatory countries) was not able to ratify the UPCA. However, only a couple of months after this decision, the Parliament and the Federal Council adopted the approval act with the required two-thirds majority. A further constitutional complaint against the approval act is still pending. In the meantime, the Federal Constitutional Court has in preliminary proceedings already decided that the complaint is obviously inadmissible.[21] Germany was finally able to ratify the UPCA and deposited its ratification deed with the Registry of the UPC on February 17, 2023, enabling the UPC to start on June 1 (*cf*. Art. 89 UPCA).

After the threshold of the required number of signatories was met in January 2022, a pertinent question remains, namely whether the withdrawal of the United Kingdom from the EU ("Brexit") will have a detrimental effect on the start of the UPC system. While it has been debated whether the UK can still be a

20. BVerfG, 2 BvR 739/17 (German Federal Constitutional Court Feb. 13, 2020), https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/02/rs20200213_2bvr073917en.html.

21. BVerfG , 2 BvR 2216/20. (German Federal Constitutional Court June 23, 2021), https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2021/06/rs20210623_2bvr221620en.html.

member of the system even after Brexit,[22] the actual problem is that the UK withdrew its previous ratification of the UPCA and its signature of the so-called Protocol to the Agreement on a Unified Patent Court on provisional application ("PAP-Protocol").[23] The PAP-Protocol is pivotal for the entering into force of the EU Patent Package. According to the PAP-Protocol, however, the United Kingdom is explicitly listed as a necessary signatory. Nevertheless, without even addressing this potential pitfall, the Council of the European Union simply declared that the PAP-Protocol entered into force in January 2022.[24] It remains to be seen whether this declaration will carry the day at the end of the first proceedings before the newly created UPC, where it can be expected that the losing parties will challenge the decisions before any available national or supranational courts.

The three main instruments setting up and defining the details of the UPC system—the UPCA, the Statute of the Unified Patent Court,[25] and the Rules of Procedure of the Unified Patent Court[26]—will likely have to be applied in the first "real" cases for the first time with the launch of the UPC. Apart from this, provisions in EU regulations already in force will also be applicable, e.g., the Unitary Patent Regulation governing translations

22. Ansgar Ohly & Rudolf Streinz, *Can the UK Stay in the UPC System after Brexit?*, 12(3) J. OF INTELL. PROP. L. & PRAC. 245 (2017), https://doi.org/10.1093/jiplp/jpx006.

23. Council of the European Union, Protocol to the Agreement on a Unified Patent Court on provisional application (PPA) (Jan. 19, 2022), https://www.consilium.europa.eu/en/documents-publications/treaties-agreements/agreement/?id=2015056.

24. *Id.*

25. *UPC Agreement*, *supra* note 16, Annex I.

26. Rules of Procedure of the Unified Patent Court, [hereinafter UPCA RoP] (July 8 2022), https://www.unified-patent-court.org/sites/default/files/upc_documents/rop_en_25_july_2022_final_consolidated_published_on_website.pdf.

of EP-UEs[27] or Recast Brussels I concerning the enforcement of decisions.[28]

Every aspect of patent litigation and civil procedure will be the subject of intense discussions in the first few years of the forthcoming UPC before any sort of established case law is developed.

27. *EU Translation Regulation*, *supra* note 18.

28. Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters (recast), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32012R1215 [hereinafter *Recast Brussels I*].

II. PATENT LITIGATION IN EUROPE AFTER IMPLEMENTATION OF THE UPC SYSTEM

A. Filing and prosecution strategies under the UPC legal framework

When the Unified Patent Court (UPC) system comes into force, all patents granted by the European Patent Office (EPO) will fall, in principle, under the jurisdiction of the UPC. However, for a transitional period of a minimum seven years after the initialization of the UPC,[29] European Patent owners or applicants[30] will have the right to "opt out" of the UPC system for their existing EPs or EP applications, i.e., declare that they do not wish the UPC to have jurisdiction over a given patent or application. "Opt-outs" can be declared within the mentioned transitional period at any time until one month before the end of the transitional period.[31] The opt-out remains valid for the entire lifetime of the patent, unless withdrawn.[32] An opt-out can

29. This seven-year period is extendable for another seven years to a maximum of fourteen years. *UPC Agreement*, *supra* note 16, Art. 83(3) and (5).

30. According to Rule 5(1) UPCA, the "proprietor" of an EP or the "applicant" of an EP application may file the opt-out with the Registry of the Court (of the UPC).* Rule 8(5)(a) and (b) UPCA stipulate that the material owner is considered "proprietor" or "applicant" (even if not registered). However, Rule 8(5)(c) UPCA provides for a rebuttable assumption that the registered person is the material owner. UPCA ROP, *supra* note 26.

* The Registry of the Court is located at the Court of Appeal in Luxembourg and has subregistries at every division of the Court of First Instance. The Registry plays a key role in the functioning of the Court. It fulfills administrative and procedural tasks for the Court and is led by the Registrar. More detailed information can be found here: https://www.unified-patent-court.org/en/registry/presentation.

31. *Id*.

32. According to Rule 5(7) UPCA, the opt-out can be withdrawn after which case a renewed opt-out is no longer possible, *cf.* Rule 5(10) UPCA. UPCA ROP, *supra* note 26.

only be declared if there is no pending action involving the underlying patent.[33]

EP applicants have some important strategic decisions to make during and after the end of the transitional period, including determining which patents should be opted out of the UPC system, whether to file divisional applications, and whether one or more divisionals should be opted out of the system. Some patent family members might be left in the system while opting out others.

Furthermore, the EP applicant might have the option of applying for a "double protection," securing patent protection as both a European Patent and as a national patent. The EPC leaves it to each contracting state to regulate whether and under what conditions an invention contained in both an EP application or an EP and a national patent application or a national patent with the same filing or priority date can be protected.[34] For example, the German and French legislatures to date—before the implementation of the UPC—have opted for a prohibition of double protection, so granted European Patents currently still trump granted German or French patents.[35] With respect to the UPC system, however, the German and French legislatures have abolished the prohibition of double protection,[36] so that EP

33. *Id.*, Rule 5(6).

34. *EP Convention*, *supra* note 9, Art. 139(3).

35. Accordingly, a national German or French patent having the same priority as the EP, to the extent that it protects the same invention as the EP, shall cease to have effect from the date on which the time limit for filing an opposition against the EP has expired without opposition having been filed, or the opposition proceedings having been finally concluded with maintenance of the EP, or the national German patent having been granted after these two dates.

36. *Cf.* German Law regarding International Treaties in the matter of patents (IntPatÜG), Art. II, § 8.

applicants will then be free to apply for a non-opted-out EP in parallel to a national patent once the UPC comes into force.[37]

Another issue to be decided by patent proprietors is whether to file their applications as European Patent with unitary effect (EP-UE) applications. According to a decision by the President of the EPO, the grant of an EP can be delayed upon request by the EP applicant so that the grant will only be published on or immediately after the date of entry into force of the UPCA.[38] This possibility is open to EP applicants once Germany will have deposited its instrument of ratification of the UPCA.[39] EP-UEs have the disadvantage that no "opt-out" is possible for them.

A more basic consideration for whether to file a request for EP-UE protection is monetary. The "cost/coverage" ratio of EP-UEs is attractive, provided that the coverage in all or a sufficient majority of the (initially) seventeen member states of the UPCA is really needed. Most EPs are validated in France, Germany, and the UK only, and the latter is not part of the UPC system.

Additionally, when deciding on whether to apply for an EP-UE, the possibility to "thin out" (i.e., allowing some designations to lapse) is no longer available. With EP-UEs, it is "all-in or all-out," i.e., a selective choice of coverage to save costs is impossible.

---

37. Amendment to the German Law regarding International Treaties in the matter of patents by law of August 20, 2021, GERMAN LAW GAZETTE, part I, pg. 3914.

38. *See* Decision of the President of the European Patent Office dated 22 December 2021 concerning the forthcoming introduction of the Unitary Patent and the possibility of requesting a delay in issuing the decision to grant an EP in response to a communication under Rule 71(3) EPC Official Journal (Jan. 2022), https://www.epo.org/law-practice/legal-texts/official-journal/2022/01/a4.html.

39. *Id*.

A cost factor that weighs in favor of pursuing an EP-UE is the savings in translation and national validation procedures. Apart from the second language, no further translations are needed, and costs for national representatives can be avoided.

B. National patent litigation in parallel to UPC patent litigation

The procedural framework established by the UPCA creates multiple opportunities for an interaction or conflict between proceedings before national courts and before the UPC. This interaction—especially, but not restricted to the transitional period—can give rise to an issue of *lis alibi pendens*, which is a principle of comity in private international law that addresses the problem of potentially contradictory judgements in two parallel proceedings. *Lis alibi pendens* permits a court to refuse to exercise jurisdiction when there is parallel litigation pending in another jurisdiction over the same matter.

1. International jurisdiction of the UPC and *lis alibi pendens*

a. International jurisdiction pre-implementation of the UPC

The framework for determining international jurisdiction for patent cases that has been in place in Europe to date—before the implementation of the UPC—is set forth in the Recast Brussels I regulation of the EU and the Lugano convention.[40] These

40. The Lugano Convention [hereinafter *Lugano Convention*], signed in 2007, provides for mutual recognition and enforcement for a wide range of civil and commercial judgements between EU and European Free Trade Association (EFTA) member states. *Available at* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A22007A1221%2803%29. The EFTA is a regional trade organization established in 1960 consisting of four European states: Iceland, Liechtenstein, Norway, and Switzerland. *See* https://eur-lex.europa.eu/EN/legal-content/glossary/european-free-trade-association-efta.html.

delineate the circumstances according to which a later seised national court of an EU member state has to stay its proceedings until such time as the jurisdiction of a first seised national court[41] of another EU member state is established:

Two courts from two different member states dealing with . . .	**Application of *lis alibi pendens*:**
Same cause of action and same parties (e.g., a typical torpedo-scenario—a Declaration of Non-infringement (DNI)-action before one court and an infringement action before a second court).	Mandatory stay of later proceedings until jurisdiction of first action is decided.[42]
Related actions (e.g., a FRAND-determination proceeding before one court and an infringement proceeding before a second court where the FRAND-objection is raised as a defence).	Discretionary stay of the later proceeding until jurisdiction is decided in the first proceeding.[43]
Exclusive jurisdiction of several courts.	No jurisdiction for the later seised court.[44]

41. The court first "seised" is the court in which proceedings are first commenced. The court later seised is the court in which proceedings are subsequently commenced.

42. *Recast Brussels I*, *supra* note 28, Art. 29(1); *Lugano convention*, *supra* note 40, Art. 27(1).

43. *Recast Brussels I*, *supra* note 28, Art. 30(1); *Lugano convention*, *supra* note 40, Art. 28(1).

44. *Recast Brussels I*, *supra* note 28, Art. 31(1); *Lugano convention*, *supra* note 40, Art. 29(1).

b. International jurisdiction post-forthcoming implementation of the UPC

In the runup to the establishment of the UPC, the Recast Brussels I regulation was amended to include Articles 71a–d dealing with the relationship between national courts of EU member states and the UPC. The UPC is treated as a court of an EU member state.[45] The above outlined provisions of Recast Brussels I apply when both an (ordinary) court of an EU member state and the UPC are seised.[46] The international jurisdiction of the UPC is now prescribed as follows:[47]

- The UPC has (international) jurisdiction if any local court of a UPC member state has international jurisdiction.[48] [49]
- If a defendant is not domiciled within the EU:[50]
    - International jurisdiction is determined pursuant to Art. 4 et seq. Recast Brussels I irrespective of the defendant's domicile.

45. *Recast Brussels I*, *supra* note 28, Art. 71a

46. *Id.*, Art. 71c.

47. *Id.*, Art. 71b.

48. *Id.*, Art. 71b(1).

49. In this regard, it could be argued that in all instances where a local court of any EU member state would accept jurisdiction based on its private international law rules, the UPC could also accept jurisdiction. For example, Belgian, French, and Luxemburg national laws principally always allow its nationals to seise a national court against non-EU nationals, which could potentially open the floodgates for cross-border injunctions. However, the EU legislator expressly aimed at ruling out this possibility and clarified that the UPC should establish a "close connection" between the respective proceedings and the territory of the EU member state concerned (*cf.* recital 6 of Regulation 542/2014).

50. *Recast Brussels I*, *supra* note 28, Art. 71b(2).

  - Preliminary measures[51] by the UPC are admissible even if the courts of a third state (i.e., a non-EU member state) have international jurisdiction regarding main actions.

- The UPC may have international jurisdiction for damages outside the EU.[52]

With this in mind, a first layer of possible interaction is inherent in the jurisdictional framework established by the provision of a transitional regime under Article 83 UPCA, which implies that non-opted-out EPs will be subject to the dual jurisdiction of both the UPC and national courts.[53] Given the dual jurisdiction that exists for non-opted-out patents during the transitional period, there are basically four pathways for prosecuting and litigating patents in member states of the UPCA during the transitional period:

---

51. According to the Court of Justice of the European Union's understanding of this term, provisional measures are characterized by the fact that they are intended to prevent a change in the factual or legal situation in order to safeguard rights the recognition of which is otherwise sought before the court having jurisdiction as to the substance of the matter, cf. Reichert & Ors v Dresdner Bank AG, C-261/90 (E.C.J. 1992)), https://eur-lex.europa.eu/resource.html?uri=cellar:2b8ccc17-ef91-4757-a5d6-d62e870c490f.0002.06/DOC_1&format=PDF.

Accordingly, the term "preliminary measures" has a broad scope and includes, e.g., proceedings regarding preliminary injunctions, seizure of goods suspected of infringement, and the freezing of bank accounts or other assets. *See* also Chapter IV.B.8. outlining the available provisional measures before the UPC.

52. *Recast Brussels I*, *supra* note 28, Art. 71b(3).

53. *UPC Agreement*, *supra* note 16, Art. 83(1).

Pathway	Filing Office	Validation[54]	Opt-out	Litigation venue
No. 1	EPO	Nationally	Yes	National courts
No. 2 EP-UE	EPO	Nationally	No	UPC / National courts
No. 3	EPO	European Patent with unitary effect	Not possible	UPC
No. 4	National Patent Offices	n/a	n/a	National courts

While the first two options will no longer be applicable after the end of the transitional period in certain countries where EPs and national patents may no longer coexist, some countries (e.g., Germany) will still allow for double patent protection with respect to EP-UEs. Additionally, some contracting member states (e.g., France and the Netherlands) have closed the "national route" by entering the Patent Cooperation Treaty,[55] under

54. EP validation is the process of converting a single EP Application upon grant into at least one national patent or into a bundle of one or more of the 44 EPO member, extension, and validation states. For EP-UEs, the validation covers the territory of the UPC member states only as of the date of validation. Therefore, an expansion of the UPC area after the validation of a given EP-UE will have no effect on the territorial scope of this EP-UE, so different EP-UEs may have different territorial scopes.

55. The Patent Cooperation Treaty was signed in the 1970s to provide an economical and streamlined means for the filing of patent applications in several countries. It is governed by the World Intellectual Property Organization and has more than 150 nations as signatories.

which international patent applications cannot be nationalized at those members states' national patent offices.

i. Opting out of the UPC system

For patent proprietors, the question whether to opt out of the UPC system for their existing EPs or EP applications is a key strategic decision in preparing for implementation of the UPC. There are two types of opt-outs to choose from: 1.) a "preemptive" opt-out, filed before any action is taken in the case and 2.) an opt-out on a case-by-case basis, filed only after an infringement is identified.

By choosing a preemptive opt-out, the proprietor ensures that competitors do not have the opportunity to block the opt-out by filing a nullity suit before the UPC.[56] Also, since opt-outs can be withdrawn (unless an action has already been brought before a national court[57]), proprietors may still ultimately choose the UPC as their venue.

Disadvantages of choosing a preemptive opt-out include the upfront decision-making and administrative effort required to opt out, the inability to make use of all the advantages of the new system (e.g., the injunction leverage of the broad territorial scope,[58] the rocket docket of the UPC,[59] as well as the attractive cost reimbursement system[60]), and the risk of the proprietor being entirely locked out of the UPC system if a potential

56. Another way to achieve the same ends is the patent owner might take advantage of any national bifurcation where applicable (e.g., Germany). By doing this, the patentee can avoid any risk of a counterclaim of revocation in infringement proceedings.

57. *UPC Agreement*, *supra* note 16, Art. 83(4).

58. *See infra* Section II.B.2 ("Torpedo" actions) for details.

59. *See infra* Section III.B (Case management of UPC litigation) for details.

60. *See infra* Section IV.I (Cost awards before the UPC) for details.

defendant files a preemptive action before a national court before the proprietor can withdraw its preemptive "opt-out."

By choosing to opt out on a case-by-case basis, the patentee benefits from not having to take the upfront administrative action to preemptively opt out. But not filing a preemptive opt-out risks being preempted by a competitor filing a nullity action before the UPC before the proprietor has the opportunity to file its opt-out, which would lock the EP in the UPC system.

By choosing to not opt out either preemptively or on a case-by-case basis, the proprietor benefits by avoiding any risk of being locked out of the UPC system by any preemptive national actions by potential defendants.

ii. Staying in (i.e., not opting out of) the UPC system

In the absence of opt-outs, proprietors and defendants will be able—during the transitional period—to bring actions in relation to non-opted-out EPs before both the UPC and the national courts.[61]

61. It has been noted that the language of Article 83(1) UPCA, albeit apparently limited to actions for infringement and revocation, should be interpreted as extending to actions for declarations of noninfringement, as well as to protective and provisional measures. A different interpretation would imply restricting the choice of forum to just one party and would pose questions of unjustified unequal treatment. *See* ANGSAR OHLY, THE JURISDICTION OF EUROPEAN COURTS IN PATENT DISPUTES 20, EUROPEAN PATENT ACADEMY (2022), *available at* https://www.epo.org/learning/materials/jurisdiction.html. For the position that the language of Article 83(1) UPCA is a shorthand for referring to any action that comes under the jurisdiction of the UPC, *see also* Alan Johnson, *Unified Patent Court*, THE PATENT LITIGATION LAW REVIEW (3rd ed. 2019), at 9, *available at* https://www.bristows.com/app/uploads/2019/12/Unified-Patent-Court-The-Patent-Litigation-Law-Review-Nov-2019.pdf, and an introductory document to the UPC prepared by the European Patent Academy of the EPO, at 20, *available at* https://e-

This flexibility generates a myriad of potential scenarios of parallel proceedings at the UPC and national level, as well as multiple opportunities for forum shopping. This is further exacerbated by the fact that a number of points regarding the relationship between such potential parallel actions on non-opted-out EPs remain uncertain, as the language of Article 83(1) UPCA leaves room for different interpretations.

A first point of uncertainty is whether actions brought before national courts in respect of non-opted-out EPs block the UPC's jurisdiction altogether or whether parallel proceedings are possible, within the limits of the *lis alibi pendens* provisions of Recast Brussels I.[62] It has been noted that the UPCA does not provide for an all-or-nothing rule, according to which, once litigation has started before a national court under UPCA Article 83(1), an EP would be taken out of the jurisdiction of the UPC entirely.[63]

This would imply the possibility of parallel proceedings before national courts and the UPC concerning the same or different portions of the same non-opted-out EP. Multiple examples can be envisaged, such as national revocation actions of the national portions of a non-opted-out EP after an infringement action has been brought before the UPC or, vice versa, a central revocation action before the UPC after an infringement action has been brought before a national court. Also, under Recast Brussels I, an action based on the same portion of a non-opted-out EP could be brought both before national courts and the UPC, if directed against different parties (e.g., a national

courses.epo.org/wbts_int/litigation/UPCAgreement.pdf (last visited Dec. 21, 2022).

62. *Recast Brussels I*, *supra* note 28, Arts. 29–32.

63. *See* OHLY, *supra* note 61, at 20 *et seq*. *See also* WINFRIED TILMANN & CLEMENS PLASSMANN, UNIFIED PATENT PROTECTION IN EUROPE: A COMMENTARY 1245 (2018). Multiple practical examples are given in both works.

infringement action of the national portion of a non-opted-out EP against one defendant, and a UPC infringement action of all national portions, including the already asserted national portion, of the same non-opted-out EP against another defendant).

The opposite view has also been expressed, relying on the language of Article 34 UPCA to exclude at least certain instances of parallel proceedings.[64] Article 34 states that decisions of the UPC shall cover all portions of EPs in force in countries participating in the UPCA. This provision is then relied on to suggest that the drafters of the UPCA wished to exclude any possibility of UPC infringement or revocation actions that did not extend to all portions of the non-opted-out EP, thereby excluding UPC jurisdiction or forcing a stay of the UPC action under Article 29 Recast Brussels I where certain portions of the same non-opted-out EP have already become the object of national actions. This interpretation of the drafters' intention underlies the current language of Rule 5.1(b) UPCA, stating that the effects of opt-outs cannot be partitioned and should instead be effective for all designations.

At the same time, it is noted that the argument may not be conclusive, as Article 34 UPCA may tolerate exceptions (e.g., in the event of licenses, different owners, prior use rights, or unpublished prior rights) and may not be a sufficiently reliable basis to exclude the possibility of parallel actions.[65] Furthermore, Article 34 would resolve only part of the problem and would not avoid the possibility of different types of actions brought before the UPC and national courts (e.g., an infringement action

64. For a reference to this possible interpretation of UPCA Article 34, *see* JUSTINE PILA AND PAUL TORREMANS, EUROPEAN INTELLECTUAL PROPERTY LAW 643 (2016).

65. *Cf.* TILMANN & PLASSMANN, *supra* note 63.

before the UPC and revocation actions before the national courts).

In essence, the issue is unclear and will certainly be the object of extensive litigation in the early days of the UPC. Also, no matter the solution early UPC jurisprudence will give to the above issues, it can be predicted that an unintended but likely consequence of this dual jurisdiction will be a race to the courthouse in the event of non-opted-out EPs, to seise the preferred jurisdiction before any preemptive action is filed by the other side. Also, no matter the solution adopted by the early case law of the UPC, tactical preemptive national patent litigation will most likely remain a factor, if only to shield key markets (e.g., where manufacturing takes place) from the jurisdiction of the UPC or to influence UPC proceedings (e.g., relying on the shorter time to trial before certain national courts with a view of creating infringement or validity precedents to be then relied on before the UPC). These problems will not arise for opted-out EPs (provided that the opt-out is valid), which will only be subject to the jurisdiction of the national courts.

2. "Torpedo" actions

A second layer of possible interaction between proceedings before national courts and proceedings before the UPC does not depend on the transitional regime and is inherent in the jurisdictional system under Recast Brussels I. Multiple scenarios can indeed be envisaged of parallel proceedings between the UPC and national courts involving the same cause of action between the same parties as per Article 29 Recast Brussels I or related actions as per Article 30—actions that are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgements.

The typical example of application of Article 29 would be that of so called "torpedo actions," i.e., noninfringement actions

filed before a national court in a noncontracting member state, seeking a declaration of noninfringement (DNI) of a patent that is subject to the jurisdiction of the UPC. As the UPC is deemed to be a court of the contracting member states and is subject to the same obligations under EU law as any national court of the contracting member states,[66] the above *lis alibi pendens* rules of Article 29 apply. Outside the UPC system, a patentee could at least to some extent counter this DNI torpedo by filing a request for preliminary injunction, because Article 35 Recast Brussels I excludes preliminary measures from the *lis alibi pendens* provisions. However, it is not clear whether Article 35 is applicable with respect to the UPC.[67] Accordingly, it might not be possible to respond to a DNI torpedo by filing a request for preliminary measures.

Additional scenarios may arise in situations where the jurisdiction is split among national courts and the UPC, depending on the form of action. By way of example, the UPC has jurisdictions over "related defences" in infringement actions, "including counterclaims concerning licenses."[68] Such defences may also be the object of main actions before national courts. Again, multiple fact patterns can be envisaged. Immediate examples would include main actions before national courts requesting a declaratory judgement that certain acts are covered by a license or exhaustion or main actions before national courts where the

66. *UPC Agreement*, *supra* note 16, Art. 1.

67. The background for this uncertainty is Article 71c *Recast Brussels I*, *supra* note 28, which with respect to the UPC only refers to Articles 29–32 (i.e., the *lis alibi pendens* rules as outlined above) but expressly not to Article 35. To the extent that Article 71b(2) provides for a similar possibility to file requests for preliminary measures, this provision is (at least based on a literal interpretation) only applicable if a non-EU court accepted jurisdiction for the corresponding main action.

68. *UPC Agreement*, *supra* note 16, Art. 32(1)(a).

seised court is asked to establish the terms of a license in a competition law or FRAND setting. If the same issue is then brought before the UPC as a defence to an infringement action, the UPC may conclude that UPC proceedings should be mandatorily or discretionarily stayed.[69]

3. The long-arm jurisdiction of the UPC

Based on the above outlined rules on international jurisdiction for the UPC, this court is also vested with long-arm jurisdictional powers.

Recast Brussels I grants the UPC the power to issue preliminary measures even if the courts of non-EU member states have international jurisdiction with respect to main actions.[70] In other words, the UPC has jurisdiction for preliminary measures even if it itself did not have jurisdiction over the main action. Accordingly, this provision could arguably open the doors for cross-border preliminary injunctions with effect in non-EU European Patent Convention members states (e.g., Turkey).[71]

Besides, the UPC may award damages for acts of infringement of EPs that are in force outside the EU.[72] This is new terrain

69. Such a stay would be pursuant to either Article 29 *Recast Brussels I*, *supra* note 28 (if its application is not viewed to be excluded by Article 71(c)(1)) or pursuant to Article 30 *Recast Brussels I* and the general principles governing the *Brussels* regime, driven by the need to avoid irreconcilable judgements.

70. *Recast Brussels I*, *supra* note 28, Art. 71(b)(2).

71. The point is controversial, as Art. 71(b)(2) has to be reconciled with the language of Recital 33 of *Recast Brussels I*, which provides that: "where provisional, including protective, measures are ordered by a court of a Member State not having jurisdiction as to the substance of the matter, the effect of such measures should be confined, under this Regulation, to the territory of that Member State." It can be predicted that the uncertainty will need to be resolved by the CJEU when the first cases arise.

72. *Id.*, Art. 71b(3).

for EU courts that, prior to the establishment of the UPC, could only award damages for acts of infringement occurring on their respective territory. Nevertheless, this provision is unlikely to gain much ground, as the hurdles are very high (infringement must occur within the UPC, some property of defendant must be located within a UPC member state, the extra territorial infringement must give rise to damages within the EU, and the dispute must have "sufficient connection" with UPC member state where property is located), and this provision is not applicable to defendants located in the area of the Lugano convention.[73]

4. Double patenting

A further layer of possible interaction between proceedings before national courts and proceedings before the UPC derives from the possibility of retaining national patent or utility model rights in parallel with European Patents or European Patents with unitary effect (EP-UEs).[74] The coexistence of EPs or EP-UEs with national rights will allow patentees to bring parallel actions before the UPC and the national courts.

One may wonder whether the UPC or the national courts may wish to reduce the risk of inconsistent decisions (and avoid a duplicative use of judicial resources) by relying on discretionary stays under Article 30 Recast Brussels I.[75] The legal basis for doing so would require some creative effort, however, as from a formal perspective, the risk of irreconcilable judgements does

73. Article 73(1) *Recast Brussels I*, *supra* note 28, stipulates the primacy of the *Lugano convention*, *supra* note 40, which does not allow for a corresponding long-arm jurisdiction.

74. *See supra* Section II.B.1 (International jurisdiction of the UPC and *lis alibi pendens*) for the various possibilities of double patenting recognized by various contracting member states.

75. *Id*.

not exist when the causes of actions (the infringement of the European right and that of the national right) are not related.

If discretionary stays do not become an issue, the existence of parallel rights over the same invention will become another source of tactical litigation for pan-European litigation strategies, multiplying the venues where remedies are sought in hopes of creating influential precedents to be exported in the parallel jurisdiction or reducing the risk of enforcement.

Also, national litigation may be resorted to in situations where it provides tactical advantages, e.g., allowing for broad pretrial discovery measures (as is the case in, e.g., France and Italy with the orders for "*saisie-contrefaçon*" or "*descrizione*" respectively, enabling the holding of an intellectual property right to have the claimed violation of these rights recorded by a bailiff authorized to enter any place where the infringement might be observed and seize the items of evidence of the infringement) or preliminary injunctions before grant (as is possible in Italy on the basis of national or EP applications).

5. No obligation to concentrate all patents in one action before the UPC

In this regard, patentees should take into consideration that unlike the rules of procedure in some participating EU member states, including Germany,[76] the UPCA does not require the patentee to include all patents that it considers infringed by a certain product or process in the statement of claims. Thus, the patentee may get a "second bite at the apple" of filing for infringement in the UPC system based on a patent that may otherwise be barred from enforcement due to the aforesaid national

76. Patentgesetz [PatG] [German Patent Act], Dec. 16, 1980, § 145 (*Zwang zur Klagekonzentration*), https://www.gesetze-im-internet.de/englisch_patg/englisch_patg.html.

rules, and the defendant has no available defence on this ground.

C. *The impact of the UPC system on licensing and tech-transfer agreements*

Licensing and tech-transfer agreements are typically broadly drafted and often include provisions on the (co-)ownership of patent applications and patents, prosecution, and enforcement. However, with the new UPC system and the Unitary Patent Regulation implementing enhanced cooperation in the creation of unitary patent protection, some details may need to be addressed in future agreements or may require reconsideration in existing agreements.[77] Particularly, existing agreements are unlikely to have addressed who may decide to register an opt-out or withdraw an opt-out, but this is often a crucial point for exclusive licensees.

For the question of who can bring an action before the court, the UPC system distinguishes three different parties: the proprietor, the exclusive licensee, and the nonexclusive licensee. In the UPC system, the patent proprietor is prima facie entitled to bring actions before the court.[78] The holder of an exclusive license is entitled to bring actions under the same circumstances as the patent proprietor, provided that prior notice is given to the proprietor.[79] This right, however, is not given to nonexclusive licensees. The holder of a nonexclusive license is only entitled to bring actions before the court in so far as it is expressly permitted in the license agreement.[80] In addition, the same prior notice obligation as exists for exclusive licensees applies to

77. *See Unitary Patent Regulation, supra* note 17.

78. *UPC Agreement*, *supra* note 16, Art. 47(1).

79. *Id.*, Art. 47(2).

80. *Id.*, Art. 47(3).

nonexclusive licensees. Since litigation in the UPC system is likely not expressly mentioned in existing licensing and tech-transfer agreements, this requires a review of the agreements.

Moreover, in any action brought by a licensee, e.g., infringement or a declaration of noninfringement, the proprietor can join the action.[81] The latter is even a requirement if the validity of the patent is challenged.[82] How to deal with the proprietor joining the action in existing license agreements needs to be reviewed.

A complicating factor is that the party who is entitled to bring an action before the court may be at odds with the party who is entitled to opt out or withdraw the opt-out. In principle, only the proprietor may opt out or withdraw the opt-out,[83] meaning the licensee cannot control this. There can be a conflict if the (exclusive) licensee has the right of enforcement but cannot decide where to bring an action because of a lack of control over the registration or withdrawal of an opt-out. This situation requires coordination between a licensee and the proprietor that may be easier to achieve if it is addressed before the prospect of any litigation. To address this preemptively may be straightforward for new agreements but may require (re)negotiation for existing agreements. For tech-transfer agreements, it is just as important for parties to consider the opt-out, as it is a joint action.[84] Parties could choose a joint opt-out; or they could choose to have the opt-out determination lie with the party entitled to file the patent and impose a duty to cooperate on the other party.

---

81. *Id.*, Art. 47(4).

82. *Id.* Art. 47(5).

83. Rule 5, UPCA RoP, *supra* note 26.

84. *Id.*, Rule 5(1).

Parties should also consider the provisions of the Unitary Patent Regulation.[85] The Unitary Patent Regulation determines that the holder of an EP-UE has the option to file a statement at the European Patent Office to the effect that the proprietor is prepared to allow any person to use the invention as a licensee in return for appropriate consideration. The license will be treated as a contractual license.[86] Further, if parties cannot agree on the appropriate consideration, the UPC has exclusive competence to establish this.[87] This competence is somewhat remarkable: on the one hand, the court can determine what a reasonable compensation (or royalty) would be for a license of right, but on the other hand, it will not have competence, at least as the object of a main action, to determine a FRAND royalty (as this is not included in Article 32 UPCA).

The Unitary Patent Regulation confirms that an EP-UE confers on the proprietor the right to prevent any third party from committing acts throughout the participating member states.[88] The acts that are prescribed are defined by the national law that is applicable to the patent.[89] An EP-UE shall be treated in all participating member states as a national patent of member states whose law is applicable to the patent.[90] This applicable law is cascaded, i.e., determined on an "if–then–else"-basis:[91] First ("*if*"), the applicable law would be that of the member state (a) where the EP applicant has his residence or principal place of

85. *See supra* note 17.

86. *Id.* at Art. 8(2).

87. *UPC Agreement*, *supra* note 16, Art. 32(h).

88. *See Unitary Patent Regulation*, *supra* note 17, Art. 5

89. *Id.* at Art. 7; *see also* the confluence with *UPC Agreement*, *supra* note 16, Arts. 25–27.

90. *Unitary Patent Regulation*, *supra* note 17, at Art. 7.

91. *Id*.

business or (b) where the EP applicant has a place of business. Secondly ("*else*"), if neither of these possibilities apply, the applicable law is determined based on the location of the EPO's headquarters, which is in Munich, so German law is applicable.[92] As such, for example, if the EP applicant has a principal place of business in the Netherlands, Dutch law would apply for determining what an infringing act is. Therefore, parties should carefully consider who is listed on a patent application, and in what order, in existing and future license and tech-transfer agreements.

Turning to the question of how national German law treats national German patents as an object of property, one has to bear the following principles in mind:

- Principle of definiteness: On the one hand, national German law requires that an assignment of rights in rem—and patents are considered to be rights in rem—needs to be "definite." This means that third parties must be put in a position to clearly and unambiguously assess which rights in rem were fully or partially assigned from one party to another. An assignment that violates this principle of definiteness is null and void.[93]
- No legal form requirement: On the other hand, national German law does not require any legal form (i.e., written form, notarization, etc.) for a valid assignment of a national patent (or any other rem right with the exception of real estate). This applies also to partial assignments or the grant of licenses. Thus, an oral agreement to

92. *Id*.

93. BÜRGERLICHES GESETZBUCH [BGB] [GERMAN CIVIL CODE], § 134.

transfer a national German patent constitutes a valid assignment. The same is true for the assignment of the right to claim a priority. However, the party who asserts in court that such oral assignment took place bears the burden of proof. It is certainly recommended to document in writing that an assignment took place (whereby the principle of definiteness needs to be observed in such written deeds).

- Fate of the sublicense if the main license lapses: Pursuant to the case law of the German Federal Supreme Court,[94] the sublicense remains in effect even though the main license lapses (e.g., if it was terminated for cause). Thus, proprietors that wish to avoid the consequences of this case law must include corresponding termination mechanisms in their licensing agreements.

D. European Patents with Unitary Effect: The need for freedom to operate in EPC countries with few validated EP patents

One of the effects of EP-UEs will be more valid patents in countries where only a fraction of granted EPs have been validated so far.[95] For example, in 2020, 133,715 European Patents were granted by the EPO. However, only 27,135 EPs were validated in Austria, which amounts to about 20 percent of the granted patents. With the introduction of EP-UEs, it is expected that the number of active EPs in countries such as Austria, Bulgaria, Estonia, and Portugal will increase drastically.

94. German Federal Supreme Court, decisions of 19 July 2012, docket no. I ZR 70/10 - *M2Trade* and I ZR 24/11 - *Take Five*.

95. For a description of patent validation in Europe, *see supra* note 54.

Accordingly, a freedom-to-operate analysis will be much more complex in these countries in the future.

Another challenge when conducting a freedom-to-operate analysis in the future is that EP-UEs will most likely have a different territorial scope, depending on the date when the EP-UE is granted. It is currently envisaged that EP-UEs will cover the seventeen member states when the UPC system comes into force. However, additional member states will likely join the unitary patent system after the start of the system. Therefore, the territorial scope of those EP-UEs, which were already requested when the UPC system started, will remain restricted to the seventeen member states initially participating (contrary to EU Trademarks and Community Designs, whose territorial scope grows or diminishes, which could readily be seen after the United Kingdom left the European Union). EP-UEs that are requested a few years later may cover more countries. Accordingly, for each EP-UE it will be necessary to check when its unitary effect was granted and which countries were covered by the respective request at the date of grant of the EP-UE.

Particularly challenging during the transitional period will be the proprietor's option to opt out of the jurisdiction of the UPC and to withdraw such an opt-out again. Thus, for example, if a specific patent is opted out of the UPC, when the freedom-to-operate analysis is conducted, an infringement analysis has to be completed in view of the case law of the respective national courts having jurisdiction. However, the proprietor of a specific patent could choose to withdraw the opt-out and file an infringement action with the UPC on the next day. If so, the case law of the UPC will suddenly be much more relevant than national case law. Accordingly, third parties who conduct a freedom-to-operate analysis will be well advised to prepare for both scenarios, i.e., under the jurisdiction of national courts and under the jurisdiction of the UPC.

Other procedural measures may also be appropriate. For example, not all national infringement courts in the participating member states accept protective letters. Thus, if the proprietor opts out a specific patent, it may not be possible for a defendant to validly file a protective letter with the competent court in a critical jurisdiction. But if the proprietor subsequently withdraws the opt-out, it may become highly advisable for the defendant to file a protective letter with the UPC. Parties conducting a freedom-to-operate analysis should monitor the opt-out status of each identified patent in order to take such appropriate procedural measures in a timely manner.

A party conducting a freedom-to-operate analysis should be mindful of the fact that specific countries may be covered twice. This is especially true for Germany, in which, to date, so-called "double protection" by an EP bundle patent and a national German patent for the same subject matter is prohibited. As such, any German patent to date automatically loses its legal effect if an EP bundle patent is granted for the same subject matter.[96] With regards to EP-UEs, however, as stated above, the applicable German law is different—Germany will uphold such a prohibition of double protection only for those EPs that were opted out according to Article 83(3) UPCA. Accordingly, in the future, it will be possible that national German patents and EP-UEs covering Germany will coexist. Thus, when conducting a freedom-to-operate analysis, it will be necessary to assess freedom to operate for the territory of Germany not only for the EP-UE but also a national counterpart that may have the same or a different scope of protection.

Additionally, in several EP member states (e.g., Germany, Austria, and France), it is possible to gain utility model

96. For discussion of double patenting in Germany, *see supra* Section II.A (Filing and prosecution strategies under the UPC legal framework).

protection in addition to patent protection for the same or a similar subject matter. Accordingly, when conducting a freedom-to-operate analysis for EP member states in the future, it will be necessary to assess freedom to operate for EP-UEs, corresponding national patents, or related national utility models. For example, due to a different scope of protection or a diverging interpretation, there may be freedom to operate with respect to one specific IP right, but not with respect to related IP rights having a similar or even identical scope of protection.

III. PROCEDURAL ISSUES BEFORE THE UPC

A. The structure of the UPC (Local, Regional, and Central Divisions)

It is safe to assume that we will see diverging case law and case management (in particular concerning the grant of term extensions pursuant to Rule 9) among the various local and regional divisions and the central division of the UPC. Inconsistencies will likely persist indefinitely, as has been the case for example in Germany, where we still witness today inconsistent case law and case management between the Regional Courts in Düsseldorf, Mannheim, and Munich. This will inevitably lead to forum shopping. One can only make an educated guess as to which of the various UPC divisions will be the most patentee-friendly forum. Nonetheless, patentees are best served identifying the main factors for determining which UPC division will be the best venue for their enforcement actions.

The following venues will be available for starting an infringement action before the UPC when implemented:

Local divisions:[97]

- Austria: Vienna
- Belgium: Brussels
- Denmark: Copenhagen
- Finland: Helsinki
- France: Paris
- Germany: Düsseldorf, Hamburg, Mannheim, Munich
- Italy: Milan
- Netherlands: The Hague

97. <Host Country>: <Seat(s)>

- Portugal: Lisbon
- Slovenia: Ljubljana

Regional divisions:

- Sweden Nordic-Baltic:[98] Stockholm, Riga, Tallinn, Vilnius

Central divisions:

- Paris, Munich

The local jurisdiction of the above divisions for the respective action is governed by Article 33 UPCA. Principally, infringement actions can be brought either before the local/regional division hosted by the contracting member state where the infringement occurs[99] or before the local/regional division hosted by the contracting member state where the defendant has its residence or place of business.[100] In case no local or regional division is competent, the action has to be filed with the central division.[101] Revocation actions, generally, have to be brought before the central division,[102] unless both parties agree to bring a revocation action before a division of their choice.[103] Additionally, any counterclaims for revocation also have to be brought before the same local or regional division.[104]

The composition of the panels of these UPC divisions will impact the outcome of a given UPC case, because each UPC judge will likely decide cases similarly to how the judge decided national litigation cases prior to becoming a UPC judge. The

98. Covering Sweden, Latvia, Estonia, and Lithuania.

99. *UPC Agreement*, *supra* note 16, Art. 33(1)(a).

100. Art. 33(1)(b).

101. *Id*.

102. Art. 32(1)(d).

103. Art. 33(7).

104. Art. 33(4) UPCA.

primary legal sources for patent law are Article 69(1)[105] European Patent Convention and Articles 1 and 2 of the Protocol on the Interpretation of Article 69 EPC,[106] but they provide only limited guidance as to the key questions of many areas of patent law, including claim construction, literal infringement, and the doctrine of equivalents.

For a detailed description of how UPC judicial panels will be composed, see Section III.C (Legal and technical judges) below.

How judicial panels are composed will have numerous potential substantive implications that will impact UPC local or regional division forum selection. For discussion, see Sections IV.A (Infringement and scope of protection) and IV.B (Available remedies in (main) infringement actions) below.

105. *EP Convention*, *supra* note 9, Art. 69(1) states: "The extent of the protection conferred by a EP or a EP application shall be determined by the claims. Nevertheless, the description and drawings shall be used to interpret the claims."

106. *EP Convention*, *supra* note 9, Protocol on the Interpretation of Article 69 EPC (Oct. 5, 1973, as revised by the Act revising the EPC of Nov. 29, 2000), https://www.epo.org/law-practice/legal-texts/html/epc/2020/e/ma2a.html#:~:text=Article%2069%20should%20not%20be,an%20ambiguity%20found%20in%20the.

B. Case management of UPC litigation

The UPC will have exclusive competence[107] in relation to EP-UEs, EPs, and Supplementary Protection Certificates[108] for various types of proceedings:[109]

- Actual or threatened infringement, including counterclaims concerning licenses[110]
- Declaration of noninfringement (DNI)[111]
- Provisional and protective measures and injunctions[112]
- Revocation/declaration of invalidity[113]
- Counterclaims for revocation/declaration of invalidity[114]
- Damages from provisional protection[115]

107. In this regard, Rule 19(7) UPCA is highly relevant according to which jurisdiction and competence of the UPC are irrevocably accepted, unless the defendant files a respective preliminary objection within one month after service of the complaint (Rule 19(1) UPCA). *UPC Agreement*, *supra* note 16.

108. *Id.*, Art. 3(a)–(d). Supplemental Protection Certificates (SPCs) are a European IP right that extends the duration of certain rights associated with certain patents after expiration. SPCs are available for various regulated, biologically active agents and were introduced to encourage innovation in certain fields for which regulatory approval requires an extended period of time—namely pharmaceuticals.

109. *Id.*, Art. 32.

110. *Id.*, Art. 32(1)(a).

111. *Id.*, Art. 32(1)(b).

112. *Id.*, Art. 32(1)(c).

113. *Id.*, Art. 32(1)(d).

114. *Id.*, Art. 32(1)(e).

115. *Id.*, Art. 32(1)(f).

- Use of invention prior to grant/prior user rights[116]
- Compensation regarding licenses of right under Article 8 of EU Regulation 1257/2012[117]
- Decisions of the EPO[118]

These proceedings can be divided into three phases: written, interim, and oral procedures.[119]

As the name suggests, the written procedure consists of the exchange of legal briefs, starting with the statement of claim. A patentee has to include in its statement of claim all arguments and evidence that it wishes to rely on in the proceedings. This means that all the exhibits needed to prove the position taken (e.g., that there is infringement or that the patent is invalid) have to be available and submitted at the start of the proceedings. In other words, the proceedings are "front-loaded." It is important to consider what has to be included before proceedings are started and how to best deal with the front-loaded approach, as it might be difficult to bring in further information or file requests in the course of the proceedings. A change of claim or amendment of a case requires an explanation why the change or amendment was not included in the original pleading and may be rejected by the court.[120]

The interim procedure[121] goes hand in hand with the stipulated active case management by the court.[122] In this stage of the

116. *Id.*, Art. 32(1)(g).

117. *Id.*, Art. 32(1)(h).

118. *Id.*, Art. 32(1)(i).

119. *Id.*, Art. 52, and Rule 10, UPCA ROP, *supra* note 26.

120. *Id.*, Rule 263.

121. *UPC Agreement*, *supra* note 16, Art. 52(2); Rules 101 *et seq.*, UPCA ROP, *supra* note 26.

122. *UPC Agreement*, *supra* note 16, Art. 43.

proceedings, which starts after the written procedure and which shall be concluded within three months,[123] the judge-rapporteur is to prepare the oral hearing by identifying the main issues and disputes as well as clarifying the parties' positions. To achieve these goals, the judge-rapporteur has a wide range of options, including holding an interim conference and issuing the orders for which the parties are to:

- provide further clarification on specific points;
- answer specific questions;
- produce evidence; and
- lodge specific documents, including each party's summary of the orders to be sought at the interim conference.[124]

Failure to comply with these orders may result in a judgement by default.[125]

The oral procedure[126] is supposed to prepare the action for decision by oral pleadings, testimony[127] of witnesses and experts, and answers to specific questions posed by the court. The goal is to complete the (principally public) hearing within one day[128] and which may only be adjourned in exceptional cases.[129]

It is easier for the patentee, as the party that initiates the proceedings, to deal with the front-loaded approach than it is for the defendant. The difficulty for the defendant is exacerbated by

123. Rule 101(3), UPCA RoP, *supra* note 26.

124. Rule 103(1), UPCA RoP, *supra* note 26.

125. *Id.*, Rules 103(2) and 355.

126. *Id.*, Rules 108 *et seq*.

127. Arguably, Rule 112(5) UPCA allows for cross-examination of witnesses and experts.

128. *Id.*, Rule 113(1).

129. *Id.*, Rule 114.

the short deadlines laid down in the Rules of Procedure, which are in principle extendable.[130] The defendant has three months from service of the statement of claim to lodge a statement of defence in an infringement action[131] or two months in a revocation action or an action seeking a DNI.[132] If the defendant wishes to file a counterclaim for revocation or infringement, it must be included in the statement of defence.[133] In turn, any requests to amend the patent that is filed after the two-month period needs the leave of the court, and claimants should not expect the court to be very generous, at least initially. This means for both parties that diligent preparation is key to success.

The front-loaded approach of UPC proceedings impacts the division of the burden of proof and vice versa. The burden of proof of all facts shall be on the party relying on those facts.[134] Where the patentee thus relies on certain facts in its statement of claim, it needs to obtain all necessary evidence validating those facts before filing. Parties have a duty to offer or produce evidence when a statement of fact is contested or likely to be contested.[135] Article 55 UPCA provides an important reversal of the burden of proof regarding the relationship between process patents and products: without evidence to the contrary, a new product will be deemed to be obtained by the patented process if the attacked product is identical to the product obtained from the patented process. The alleged infringing party can refute the presumption with proof to the contrary, whereby its legitimate

130. *Id.*, Rule 9(3).

131. *Id.*, Rule 23.

132. *Id.*, Rules 49 and 67.

133. *Id.*, Rules 25 and 50.

134. *UPC Agreement*, *supra* note 16, Art. 54.

135. Rules 171(1) and 172(1), UPCA RoP, *supra* note 26.

interests in protecting its manufacturing and trade secrets would need to be taken into account.

The evidence can come in various forms, including particular documents, written witness statements, drawings, expert reports, reports on experiments carried out for the purpose of the proceedings, physical objects (e.g., devices, products, or models), electronic files, and audio/video recordings.[136]

When it comes to obtaining the evidence, the initiative in principle lies with the parties themselves, and the procedures thereof will be governed by the Rules of Procedure. Unlike in U.S. and (to some extent) UK litigation, UPC proceedings do not provide for a general obligation to disclose potentially relevant evidence, i.e., there are no discovery or disclosure obligations. Parties relying on facts that are contested have to produce evidence available to them in support of those facts,[137] but they do not have to produce documents or other evidence that could adversely affect their case or support another party's case. There are, however, effective ways to secure or obtain evidence, including documents and samples, that is known to exist. The types of fact-finding possibilities provided in the UPCA, such as an inspection and seizure, are described below in Section IV.G.4.d. The confluence of these possibilities with national evidence proceedings is described below in Section IV.G.5. In this context, it is useful to note that in infringement proceedings, the patentee can also lodge an application for an order to preserve evidence (also called a "*saisie*") prior to an order for inspection.[138] The court may then order prompt and effective

136. *UPC Agreement*, *supra* note 16, Art. 53, and Rule 170(1), UPCA RoP, *supra* note 26.

137. *Id.*, Rule 172.

138. *UPC Agreement*, *supra* note 16, Art. 60, and Rule 192, UPCA RoP, *supra* note 26.

provisional measures to preserve relevant evidence in respect of the alleged infringement.

Aside from the fact-finding seizure and inspection (with or without *saisie*), the means for obtaining any evidence in UPC proceedings are broad, including moving for a hearing of the parties, witnesses, or experts, moving for an order for inspection of a place or object, and moving for an order for a party or third party to produce evidence.[139]

C. Legal and technical judges

The composition of the panels of the court of first instance is regulated by Articles 8 and 19–20 UPCA and Rule 345 UPCA and varies depending on the type of division, as outlined below:

- Central division: the panel is composed of two legally qualified judges who are nationals of different contracting member states and one technically qualified judge, allocated from the pool of judges established under Article 18 UPCA.
- Regional divisions: the panel is composed of two legally qualified judges chosen from a regional list of judges, who shall be nationals of the contracting member states concerned, and one legally qualified judge who shall not be a national of the contracting member states concerned and who shall be allocated from the pool of judges.
- Local divisions: the composition of the panel varies depending on the volume of patent cases in the contracting member state hosting the local division. For contracting member states

139. *UPC Agreement*, *supra* note 16, Arts. 53(1) & 59, and Rules 170 (2)–(3) and 190, UPCA ROP, *supra* note 26.

> where less than 50 cases a year are heard on average during a period of three successive years prior or subsequent to the entry into force of the UPCA, the panel is composed of one legally qualified judge who is a national of the contracting member state hosting the local division concerned and two legally qualified judges who are not nationals of the contracting member state concerned and are allocated from the pool of judges on a case-by-case basis. For contracting member states where more than 50 cases a year are heard, the panel is composed of two legally qualified judges who are nationals of the contracting member state hosting the local division concerned and one legally qualified judge who is not a national of the contracting member state concerned and who is allocated from the pool of judges. (This currently applies to the local divisions in Düsseldorf, Hamburg, Mannheim, Munich, Paris, The Hague, and Milan.) The allocation from the pool of judges may be on a case-by-case or permanent basis, depending on the workload of the court and the need to have a permanently sitting panel to handle the workload of the division.[140]

Any panel of a local or regional division may, after having heard the parties, submit ex officio a request to the president of the court of first instance to allocate from the pool of judges an additional technically qualified judge with qualifications and experience in the field of technology concerned, where it deems

140. *UPC Agreement*, *supra* note 16, Art. 8(3).

this appropriate.[141] This request of allocation of a technically qualified judge is compulsory in the event of counterclaims for revocation when the local division decides to hear both the infringement and invalidity claims.[142]

This request of allocation of a technically qualified judge can also be raised by the parties. Upon request by one of the parties, any panel of a local or regional division shall request the president of the court of first instance to allocate from the pool of judges an additional technically qualified judge with qualifications and experience in the field of technology concerned.[143]

The request to allocate a technical judge could play an important strategic role under a number of perspectives:

- Requesting the allocation of a technical judge would increase the technical expertise of the panel, which may be a factor to consider in cases raising complex technical questions (the patentee may, e.g., perceive that the presence of a technical judge might be beneficial in a case of infringement by equivalents, as a technical judge may be more willing to focus on technical functions; while a defendant may, e.g., perceive that the presence of a technical judge might be

141. *Id.*, Art. 8(5).

142. *Id.*, Art. 33(3)(a).

143. *Id.*, Art. 8(5), and Rule 3, UPCA ROP, *supra* note 26. Based on the language used by the relevant provision of the UPCA ("shall"), the court has no discretion in processing the request. This principle is balanced, however, by Rule 33, under which a request to appoint a technical judge shall be lodged as early as possible in the written procedure, and if it is lodged after the closure of the written procedure, it shall be granted only if justified in view of changed circumstances, such as new submissions presented by the other party and allowed by the court.

beneficial to address certain grounds of invalidity).

- Requesting the allocation of a technical judge might also be an effective tool for the defendant to reduce the perceived potential risk of bifurcation before local or regional divisions (especially in the early phases of UPC jurisprudence, in the absence of established case law on the point).[144] Faced with an early request to allocate a technical judge in a case where a counterclaim for revocation is filed, coupled with an indication that such request is not conditional on the counterclaim, the local or regional division might indeed have an incentive to proceed with both the action for infringement and the counterclaim for revocation.[145]
- Lastly, requesting the allocation of a technical judge might serve the purpose of balancing (or, contrarily, further increasing) the influence of a specific legal tradition or approach among the legal judges composing the panel at hand, depending on the language of the proceedings and the formation of the panel.

The allocation of judges from the pool of judges is done by the president of the court of first instance on the basis of "their legal or technical expertise, linguistic skills and relevant experience."[146] Linguistic skills play an important role in the selection of judges to be allocated, as the judge to be allocated will need to be skilled in the language of the proceedings (or in the

144. *UPC Agreement*, *supra* note 16, Art. 33(3)(c).

145. *Id.*, Art. 33(3)(a).

146. *Id.*, Art. 18(3).

language used by the division, if the allocation is permanent). This means that for proceedings conducted in languages other than English, the judge to be allocated will likely be a national of the seat of the concerned local or regional division.

Any panel of the court of appeal shall be a multinational composition of five judges.[147] It shall include three legally qualified judges who are nationals of different contracting member states and two technically qualified judges assigned from the pool of judges by the president of the court of appeal.[148]

The role of the technical judges in the decision-making process of the panels where they sit might be interpreted differently depending on the nationality of the judges of that panel and their experience with their own national judicial systems. The national courts of certain contracting member states are used to appoint technical advisors. Their involvement varies depending on the practice of the individual jurisdiction and can range from the preparation of an opinion for the court on all issues of validity or infringement (e.g., in Italy) to the provision of opinions on individual technical points (e.g., in Austria and Belgium).

Local divisions in contracting member states having a tradition with technical advisors might be inclined to request the appointment of technical judges even in the absence of requests from the parties and might be inclined to give significant weight to the opinion of the technical judge. Also, they could consider requesting technical judges to prepare concise preliminary opinions for the panel, e.g., in preparation of the oral proceedings.[149] A closer involvement of technical judges in the

147. *Id.*, Arts. 9 and 21, and Rule 345, UPCA RoP, *supra* note 26.

148. *Id.*

149. A similar interaction characterizes proceedings before the Swiss Federal Patent Court, one of the few examples of a court having a similar architecture, with panels composed of legal and technical judges.

assessment of matters of validity may increase the influence of EPO practice in the assessment of inventive step in the local divisions in questions. This is because technical judges are in large part patent attorneys, who typically follow EPO practice.

The role and influence of technical judges might instead be more limited in contracting member states where judges traditionally decide on patent matters, including technical issues, without the support of external advisors.

Different local practices may develop in the early years of UPC jurisprudence, and it will be interesting to see how this may affect court practice and forum selection choices of the parties.

The names of the 85 judges appointed to the UPC were announced on October 19, 2022.[150] Thirty-four are legally qualified judges, and 51 are technically qualified judges. At least initially, until the docket of the court becomes more crowded over time, most of them will act on a part-time basis.

Germany (twenty-eight) and France (seventeen) have the highest number of UPC judges. Italy follows with eleven judges, and the Netherlands has seven (which makes 61 out of 85 judges coming from just four countries). Here is a full list of the nationalities of all judges currently appointed:

Country	Legally qualified judges	Technically qualified judges	Total
Germany	12	16	28
France	5	12	17
Italy	4	7	11
The Netherlands	4	3	7

150. A full list of the names of the judges appointed is published on the court's website, https://www.unified-patent-court.org/en/news/unified-patent-court-judicial-appointments-and-presidium-elections.

Country	Legally qualified judges	Technically qualified judges	Total
Belgium	1	4	5
Denmark	(1 to be appointed)	4	4
Sweden	2	2	4
Finland	1	3	4
Austria	1	0	1
Bulgaria	1	0	1
Portugal	1	0	1
Slovenia	1	0	1
Estonia	1	0	1

The court will be led by Mr. Klaus Grabinski (Germany), as President of the Court of Appeal, and Ms. Florence Butin (France), as President of the Court of First Instance.

The composition of the Presidium—the body responsible for the management of the court[151]—was also announced. In addition to the President of the Court of Appeal and the President of the Court of First Instance, the Presidium is composed of two judges from the Court of Appeal, Ms. Rian Kalden (Netherlands) and Ms. Ingeborg Simonsson (Sweden), and three judges from the Court of First Instance, Ms. Camille Lignieres (France),

151. *UPC Agreement*, *supra* note 16, Annex 1, Art. 15(3). The Presidium shall in particular draw up proposals for the amendment of the Rules of Procedure and proposals regarding the Financial Regulations of the Court; prepare the annual budget, the annual accounts, and the annual report of the Court and submit them to the Budget Committee; establish the guidelines for the training programme for judges and supervise the implementation thereof; take decisions on the appointment and removal of the Registrar and the Deputy-Registrar; lay down the rules governing the Registry including the sub-registries; and give an opinion in accordance with Article 83(5) UPCA.

Mr. Ronny Thomas (Germany), and Mr. Peter Tochtermann (Germany).

D. Bifurcated vs. nonbifurcated proceedings

Bifurcation is the ability to divide a case into two parts so as to render a judgement on a set of legal issues without looking at all aspects. In patent law, bifurcation is usually regarded as the separation of the part dealing with infringement from the part dealing with validity. The prominent example is Germany, where the infringement courts are not competent to decide on the validity of the patent. Rather, the defendant of an infringement case has to file a separate case for invalidity either before the opposition division of the EPO or the [German] Federal Patent Court. Bifurcation in Germany therefore is a decision of the legislature and cannot be handled differently by the courts.

Advocates for bifurcation would argue that decisions on validity are best left to highly specialized courts/tribunals with the appropriate technical background. A disadvantage of bifurcation, however, is the potential delay in the proceedings—namely the so-called "injunction gap," i.e., the time between the issuance of the injunction by the infringement court and the decision on validity—which can lead to an unjustified advantage for the patentee if the patent is later revoked; and inconsistencies in the claim constructions that are made independently by both courts/tribunals.

In principle, the UPC has adopted a nonbifurcated system. Article 32 UPCA specifies that the UPC is competent to decide on both infringement and validity in combination. Nevertheless, there are a couple of scenarios in which bifurcation may still take place, as follows.

1. Counterclaim for revocation following a claim for infringement[152]

A defendant may bring a counterclaim for revocation in the case of an action for infringement brought before the UPC local/regional division.[153] It is then in the discretion of the court to either proceed with both actions,[154] or to refer the counteraction for revocation to the UPC central division and then decide whether to proceed with or stay the infringement proceedings,[155] or refer both the action and the counteraction to the central division upon agreement of the parties.[156] The decision whether to refer the counteraction for revocation to the central division and also whether to proceed with or stay the infringement action is in the sole discretion of the court. Rule 37 UPCA does not provide any guidance on this question, and it remains to be seen how the case law concerning this question will develop.

2. Counterclaim for infringement following a claim for revocation[157]

In case of a counterclaim for infringement in response to a standalone action for revocation before the central division,

152. For details, *see infra* Sections III.C.9 (Revocation counteractions) and IV.D (Revocation actions).

153. *UPC Agreement*, *supra* note 16, Art. 33(3). This scenario only applies to an infringement action brought before the local or regional division. There is by default no room for bifurcation if the infringement action is brought before the central division.

154. *Id.*, Art. 33(3)(a).

155. *Id.*, Art. 33(3)(b).

156. *Id.*, Art. 33(3)(c).

157. *See also infra* Section IV.D.6 (Counterclaims for infringement / separate actions for infringement).

both infringement and revocation will be heard in combination by the central division.

The situation is more complex, however, if the patentee decides to file a separate and standalone claim for infringement before a local or regional division—the applicable provisions do not prevent the patentee from doing so (in other words, the standalone revocation claim does not lead to a *lis alibi pendens* argument). Technically, this situation would lead to a bifurcation scenario, with infringement heard before a local/regional division and revocation heard before the central division. However, such a bifurcation can be overcome if *either* both parties agree to have both claims heard before the central division[158] *or* the defendant in the infringement proceedings files a (further) counterclaim for revocation also in the infringement proceedings.[159] The local or regional division can then proceed to hear both claims in combination (see above).[160] In its discretionary decision, the local or regional division shall consider how far the central division's revocation action is advanced.[161] Until the local/regional division has decided whether to refer the revocation action to the central division[162] or decide both claims in combination, the central division shall stay the revocation action pending before it.[163]

158. *UPC Agreement*, *supra* note 16, Art. 33(3)(c).

159. This is possible according to Rule 75, UPCA ROP, *supra* note 26.

160. Pursuant to *UPC Agreement*, *supra* note 16, Art. 33(3)(a).

161. Rule 75, UPCA ROP, *supra* note 26.

162. *UPC Agreement*, *supra* note 16, Art. 33(3)(b).

163. Rule 75(3), UPCA ROP, *supra* note 26.

3. Actions for invalidity before the EPO and in national courts[164]

Counteractions for revocation can be filed with the UPC in parallel to opposition proceedings before the EPO,[165] and also in parallel to any national revocation action against a member of the same family that the EP-UE belongs to; in particular, a revocation action filed in the UK against the British part of the European Patent comes to mind. Accordingly, a pending infringement or revocation action before the UPC may be stayed (subject to the discretion of the court) pending the opposition before the EPO.[166] A pending revocation action against a national family member, even if the claim wording is the same, may cause the UPC to adapt the timeline of the litigation, but a formal stay seems out of the question, as the national court's decision is not binding upon the UPC. Such a scenario therefore is not one of bifurcation of the same case but rather one in which two (or more) courts in different jurisdictions are dealing with very similar subject matters. For potential defendants in suitable cases, however, it may be advisable to start such national proceedings as early as possible to create a "precedence" that the UPC judges deciding upon the validity of the EP-UE will consider.[167]

E. The importance of the language aspect under the UPC system

As outlined in Section I above, the language aspect has always been crucial in the runup to the various attempts to form

164. For details, *see infra* Section IV.D.3 (Relationship to EPO opposition proceedings).

165. *UPC Agreement*, *supra* note 16, Art. 33(8) and (10).

166. Rule 295, UPCA RoP, *supra* note 26.

167. *See also supra* Section II.B (National patent litigation in parallel to UPC litigation).

a unitary patent system. Accordingly, the drafters of the UPCA and the Rules have devised a complex system that differentiates between UPC local/regional divisions and the central division.

Before the local and regional divisions, the criteria for the selection of the language of the proceedings are as follows:

- one of the official languages of the EPO as designated by the local/regional division;[168]
- one of the official languages of the country in which the local division is situated, or a designated language of one of the countries hosting the regional division;[169] and
- the language in which the patent was granted, if parties and panel agree or by way of decision of the president of the court of first instance.[170]

A couple of compromises have been agreed upon to limit the claimant's ability to influence the language regime:[171]

- If the local or regional division provides for additional languages other than its respective official languages, the claimant may choose the language of the proceedings from any of these. However, if the defendant is only active within the local jurisdiction of the respective division, the language can only be one of the official languages. Additionally, the judge-rapporteur may order that judges may use the official language of that country in the oral hearing and for the

168. *UPC Agreement*, *supra* note 16, Art. 49(2).

169. *Id.*, Art. 49(1).

170. *Id.*, Arts. 49(3)–(5).

171. *Cf.* Rule 14(2), UPCA ROP, *supra* note 26.

judgement, whereas a translation will be provided.[172]

- The language of the central division is generally the language in which the patent was granted.[173] The language for the appeal proceedings follows the language used in the first instance unless parties agree to the language in which the patent was granted.[174]

If disputes in a language in which the patent was not granted are referred to the central division from a local or regional division, the judge-rapporteur in the central division may (but is not required to) order that the parties provide translations of all or portions of their written submissions in the language in which the patent was granted.[175]

172. Rules 14(2)(c) and 18, UPCA RoP, *supra* note 26.

173. *UPC Agreement*, *supra* note 16, Art. 49(6).

174. *Id.*, Art. 50.

175. Rule 39, UPCA RoP, *supra* note 26, for counterclaims for revocation; Rule 41(d) for infringement actions.

IV. SUBSTANTIVE PATENT ISSUES BEFORE THE UPC

A. Infringement and scope of protection

1. Introduction

Patents provide patentees with exclusivity rights for inventions that the patentee has in return disclosed to the public. Third parties are prohibited from performing unauthorised acts violating the exclusivity rights provided by the patent.

The rights conferred by a patent before the UPC courts are provided in Articles 25 and 26 of the UPC Agreement (UPCA), and the limitations to these rights are provided in Article 27 of the UPCA. Articles 25–27 are basically in line with similar provisions in the patent laws of most UPC contracting member states. Irrespective of these provisions, however, determining the scope of protection of a particular patent requires case-by-case analysis.

Case law developed nationally in the UPC contracting member states has shown that such determinations may differ between jurisdictions. The Unitary Patent Regulation states that the scope of protection provided by an EP-UE granted with the same set of claims in respect of all the participating member states shall benefit from unitary effect in the participating member states.[176] It shall provide uniform protection and have equal effect in all the participating member states.[177] The scope of that right and its limitations shall be uniform in all participating member states in which the EP has unitary effect.[178]

Thus, given the unitary effect of an EP-UE, there is a need for harmonization of the determination of the scope of

176. *Unitary Patent Regulation*, *supra* note 17, Art. 3.1.

177. *Id.* at Art. 3.2.

178. *Id.* at Art. 5.2.

protection. The question is where to find sources for a harmonized interpretation of claim scope and conferred rights.

2. Sources of law

The UPC bases its decisions on (a) European Union law; (b) the UPCA; (c) the European Patent Convention (EPC);[179] (d) other international agreements applicable to patents and binding on all the contracting member states; and (e) national law.[180]

However, neither European Union law nor the UPCA itself provides any further guidance to the interpretations of the scope of the rights conferred by Articles 25–27 UPCA in particular cases. Neither do the UPC Rules of Procedure (RoP).

The EPC states that the rights conferred by an EP shall be decided nationally in the territories in which the EP was validated, as if it was a national patent.[181] Further, the EPC makes it clear that the extent of protection of an EP shall be determined by the claims, and that the description and drawings shall be used to interpret the claims.[182]

The Protocol on the Interpretation of Article 69 EPC[183] further defines in Article 1 that the description shall be used to

179. *See id*.

180. *UPC Agreement*, *supra* note 16, Art. 24.

181. *EP Convention*, *supra* note 9, Art. 64.

182. *Id.* at Art. 69.

183. *Id.*, Protocol on the Interpretation of Article 69 EPC, *supra* note 106. Articles 1 and 2 of the Protocol state:

Art.1: Article 69 should not be interpreted as meaning that the extent of the protection conferred by a European patent is to be understood as that defined by the strict, literal meaning of the wording used in the claims, the description and drawings being employed only for the purpose of resolving an ambiguity found in the claims. Nor should it be taken to mean that the claims serve only as a guideline and that the actual protection conferred may extend to what, from a consideration of the description and drawings by a

define a position combining a fair protection for the patentee (guided, e.g., by the inventive concept appearing in the description) with a reasonable degree of legal certainty for third parties (guided by a strict literal interpretation of the claim language). Article 2 of the Protocol states that due account shall be taken of any element that is equivalent to an element specified in the claims, i.e., facilitate the application of the doctrine of equivalents. However, the EPC provides no further guidance to the interpretations of the scope of the rights conferred by Articles 25–27 UPCA in particular cases.

Thus, the best sources for guiding the determination of the scope of protection in particular cases are the case law developed in the participating contracting states. But there are substantive differences in the patent law from state to state. For example, some jurisdictions (e.g., the Netherlands) tend to give important weight to the general inventive concept disclosed in the patent when interpreting the claims. Other jurisdictions (e.g., Germany) give decisive weight to the function of particular claim features, and others (e.g., Italy) take a more literal approach and examine the skilled person's perception of the wording of the claims and the intention of the proprietor when drafting the claims.[184]

---

person skilled in the art, the patent proprietor has contemplated. On the contrary, it is to be interpreted as defining a position between these extremes which combines a fair protection for the patent proprietor with a reasonable degree of legal certainty for third parties.

Art. 2: For the purpose of determining the extent of protection conferred by a European patent, due account shall be taken of any element which is equivalent to an element specified in the claims.

184. Notable examples are the so-called "Epilady" decisions: Briefly, the underlying patent claimed a metal helical spring that was rotated around its axis, powered by an electric motor. The defendant's device used a cylindrical rod of elastic rubber, powered by an electric motor as well. When faced with the question of infringement, German and British courts came to different

Thus, it seems clear that there is a need for the Unified Patent Court to provide harmonization on approaches to claim construction. Since the central, regional, and local divisions of the UPC may (initially) be inclined to apply the version of the doctrine of equivalents with which the relevant judges are familiar, we should expect some degree of forum shopping while awaiting any final harmonization from the Court of Appeal of the UPC.

3. Functional claim construction

Assuming that the claims of a patent in dispute only read on an accused product if the claim features are construed in a broad functional way, an infringement suit enforcing such a patent may be best filed before the German local divisions. This is because the German patent trial courts—and in particular the Düsseldorf court—adopt a function-oriented claim construction approach that focuses on the technical effect of a claim feature rather than its literal meaning. In general, this claim construction approach has the most potential for establishing a wider scope of patent protection than approaches of other national courts within the EU.

4. The doctrine of equivalents

The doctrine of equivalents is recognised in all UPC member states and arguably is further specifically provided for in the Protocol on the Interpretation of Article 69 EPC.[185] Usually, the

conclusions: In Germany, the cylindrical rod was recognized as an equivalent of the spring (i.e., infringement was assumed), while in the United Kingdom, infringement was denied; *cf.* **UK:** Improver Corp. v. Remington Consumer Product Ltd [1990] F.S.R 181; **Germany:** Corp. & Sicommerce AG v. Remington Inc, Case No 2 U 27/89 (OLG 1991).

185. *EP Convention*, Protocol on the Interpretation of Article 69 EPC, *supra* note 106.

national courts have developed a series of questions to which the answers guide the determination of equivalents. Given the differences in the questions, however, the results are not always the same.

Further, it seems that the doctrine of equivalents is itself a moving target even at a national level among courts in the same jurisdiction, and as seen in, for example, the *Pemetrexed* cases,[186] courts all over Europe applying the conventional claims construction principles developed for their jurisdictions have had their decisions overturned on appeal, paving the way for new ways of interpreting claims and the doctrine of equivalents. As of today, each member state has established a different multi-factor test for deciding cases under the doctrine of equivalents. While it may be practically impossible to assess with complete confidence which of these various national approaches will lead to the most favorable result for a given case, such an assessment may still influence where the patentee should file its case. It seems that several national courts in Europe have now decided that certain limitations introduced to the claim scope during prosecution can be effectively disregarded.[187]

---

186. **Germany:** LG Düsseldorf, Urteil vom 03.04.2014 - 4b O 114/12 U, OLG Düsseldorf, Urteil vom 05.03.2015 - I-2 U 16/14, (BGH) Urteil vom 14.06.2016 X ZR 29/15; **UK:** Actavis UK Ltd & Others v Eli Lilly & Company [2014] EWHC 1511 (Pat) (15 May 2014); Actavis UK Ltd & Others v Eli Lilly & Company [2015] EWCA Civ 555; Actavis UK Ltd & Others v Eli Lilly & Company [2016] EWHC 234 (Pat); Actavis UK Ltd & Others v Eli Lilly & Company [2017] UKSC 48. **Italy:** First instance preliminary decision of the Court of Milan dated 12 Sept. 2017 in R.G. 54470/2016 reversed by the Court of Milan in R.G. 45209/2017 (dated 20 Sept. 2018); **Netherlands**: First instance decision by the District Court of The Hague (C/09/541424 / HA ZA 17-1097) reversed on appeal by decision of the Hague Court of Appeal in C/09/541424/ HA ZA 17-1097 (dated 27 Oct. 2020); **France**: Tribunal judiciaire de Paris, September 11, 2020, RG No. 17/10421; **Sweden**: Stockholm Tingsrätt (PMT-1248/18).

187. In the *Pemetrexed* cases, *id.*, a claim limitation introduced at the European Patent Office during prosecution to overcome an Article 123(2)

Even further, it seems that the determination (in time) of the relevant date (i.e., the priority date, the filing date, or the date of the alleged infringement) at which equivalents is to be determined is not harmonized throughout the national courts of Europe.

Thus, it will be interesting how the UPC decides to apply this doctrine.

5. File wrapper estoppel

With respect to claim construction in general, and also with respect to the application of the doctrine of equivalents, it will be interesting to learn the extent to which the UPC will rely on the file wrapper, created during prosecution of the patent (file wrapper estoppel), and the extent to which statements or limitations made during prosecution can be used when interpreting the claims. Several national courts, e.g., the Netherlands, France, Belgium, Sweden, and Denmark, rely extensively on the file wrapper in their claim interpretation, whereas others, e.g., Germany and Italy, do not.

How the UPC will deal with this topic is uncertain. However, it seems wise for European Patent applicants to take this into consideration during prosecution of their applications at the EPO. Similarly, it will be interesting to learn if and how statements made during a (potential) revocation action at the UPC can be used when interpreting the scope of the claims in the infringement action. And if this is indeed the case, if this has an impact on the possibility of permitting the use of file wrapper estoppel.

Absent any settled case law, in particular guidance provided by the Court of Appeals, the patent should be asserted before

---

objection was initially considered, limiting the scope with respect to equivalents, but was later disregarded throughout the national courts of Europe.

the local divisions in Düsseldorf, Hamburg, Mannheim, Milan, and Munich, or the central division in Paris and Munich, since unlike, e.g., the Netherlands or France, which generally recognizes this doctrine, Germany, and Italy do not. EP applicants are almost always unaware of any potential accused product when making narrowing arguments during patent prosecution to avoid prior art, so the availability or unavailability of a file wrapper estoppel argument can significantly impact the scope of the asserted patent and the ultimate infringement determination.

B. Available remedies in (main) infringement actions

The UPC system provides for a number of remedies, which can be classified as final remedies imposed when the court finds infringement on the merits, or as provisional measures applicable in the event of an alleged infringement. This catalogue of remedies, which corresponds with the remedies and measures stated in the Enforcement Directive,[188] is developed in the UPCA and the UPCA Rules of Procedure.

Final remedies include:

1. Permanent injunctions[189]

Where the court finds infringement on the merits, it may grant an injunction against the defendant or against the intermediary whose services are used by a third party to infringe a patent, aimed at prohibiting the continuation of the infringement. As indicated by the wording "may," the UPCA does not allow for an automatic injunction, but the imposition of a

188. Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights (Apr. 29, 2004) [hereinafter *Enforcement Directive*], https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004L0048R%2801%29.

189. *UPC Agreement*, *supra* note 16, Art. 63.

permanent injunction is in the court's discretion. Although Article 63 UPCA does not provide a corresponding provision for preliminary injunctions like Article 62(2) (where the court "shall" take into account the potential harm for either of the parties resulting from the granting or the refusal of the injunction), the court may also apply proportionality considerations here. For example, the court is required to take due account of the interest of the parties when imposing remedies[190] and to ensure that they are used in a fair and equitable manner and do not distort competition.[191] If the permanent injunction is not complied with, the defendant will be ordered, where appropriate, to pay a recurring penalty to the court.[192]

Even though Germany and Italy already have at least some forms of a proportionality test codified in their respective national patent laws, automatic injunctions are still the governing rule in both jurisdictions. In cases where an injunction might bring about appreciable hardships for the defendant, such cases should be brought before UPC divisions of the member states that are reluctant to grant exceptions to the principle of the automatic injunction. This holds true, in particular, for France, Germany, Sweden and Italy.

2. Award of damages[193]

At request of the injured party, the court shall order the defendant who "knowingly, or with reasonable grounds to know," engaged in infringing activity to pay the injured party damages appropriate to the harm actually suffered by that party

190. *Id.*, Art. 56(2).

191. *Id.*, Art. 42(2).

192. *Id.*, Art. 63(2), and Rule 354(3), UPCA RoP, *supra* note 26.

193. *UPC Agreement*, *supra* note 16, Art. 68.

as a result of the infringement.[194] The UPCA makes clear that damages are nonpunitive but aim at putting the injured party in the position it would have been in had no infringement taken place. Such damages are either calculated by taking into account all appropriate aspects (such as negative economic consequences, including lost profits of the injured party and any unfair profits of the defendant, and, in appropriate cases, elements other than economic factors, such as the moral prejudice caused to the injured party) or set as a lump sum (at least the amount of royalties or fees that would have been due).[195] It should be noted that where the defendant did not knowingly or with reasonable grounds to know engage in infringing activity, the court may nevertheless order the recovery of profits or the payment of compensation.[196]

The amount of damages may be determined in the proceedings on the merits,[197] or in subsequent proceedings.[198] In the latter case, it is important that an application for determination of damages, which may include a request for an order to lay open books, cannot be lodged later than one year from service of the final decision on the merits.[199]

Finally, it should be pointed out that the EU Translation Regulation states that in the event of a dispute relating to an alleged infringement of a EP-UE, the patentee must provide, at the request and the choice of the defendant, a full translation of the

194. *Id.*, Art. 68(2).

195. *Id.*, Art. 68(3).

196. *Id.*, Art. 68(4).

197. Rule 118, UPCA RoP, *supra* note 26; also as an interim award of damages which shall at least cover the expected costs of the procedure for the award of damages and compensation on the part of the successful party, Rule 119, *id*.

198. Rule 125 *et seq*., UPCA RoP, *supra* note 26.

199. Rule 126, UPCA RoP, *supra* note 26.

EP-UE into an official language of either the participating member state in which the alleged infringement took place or the member state in which the defendant is domiciled.[200] In its assessment, the court shall, in particular where a small or medium-sized enterprise, natural person, nonprofit making organization, university, or public research organization is concerned, take into consideration whether the defendant acted without knowing or without reasonable grounds for knowing of infringing the EP-UE before having been provided with the requested full translation.[201]

3. Communication of information[202]

On a justified and proportionate request,[203] the court may order the defendant or, under the conditions of Article 67(2) UPCA,[204] any third party to inform of (a) the origin and distribution channels of the infringing products or processes, (b) the quantities produced, manufactured, delivered, received, or ordered, as well as the price obtained for the infringing products, and (c) the identity of any third person involved in the production or distribution of the infringing products or in the use of the infringing process.[205] For the protection of confidential

200. EU Regulation 1260/2012, *supra* note 18, Art. 4(1).

201. *Id.* at Art. 4(4).

202. *UPC Agreement*, *supra* note 16, Art. 67.

203. Rule 191, UPCA RoP, *supra* note 26.

204. This applies to third parties who (a) were found in the possession of the infringing products on a commercial scale or to be using an infringing process on a commercial scale, (b) were found to be providing on a commercial scale services used in infringing activities, or (c) were indicated by the person referred to in points (a) or (b) as being involved in the production, manufacture, or distribution of the infringing products or processes or in the provision of the services.

205. *UPC Agreement*, *supra* note 16, Art. 67.

information, the court may order that this information be disclosed to certain named persons only and be subject to appropriate terms of nondisclosure.[206] In particular where the court orders a third party to provide the information, the interests of that third party shall be duly taken into account.[207]

4. Compensation[208]

The court has the exclusive competence in respect of actions for compensation derived from the provisional protection conferred by a published EP application.[209] While the UPCA does not provide an explicit legal basis for such claim for compensation, a patentee can base its claim on Article 67(1) in conjunction with Article 64 European Patent Convention. Accordingly, an EP application principally grants the applicant the same level of rights and protection as a granted patent under Article 64 from the date of its publication in the designated contracting states. In this respect, Article 67(2) EPC allows the contracting states to only grant a lower level of protection for published EP applications and even to deny the protection under Article 64 altogether, provided that comparable national patent applications do not enjoy better protection.[210] As a minimum protection, however, a "compensation reasonable in the circumstances" is to be provided so long as the third-party use of the patent application involves conduct that would be considered culpable under national law in the case of patent infringement.

206. Rules 191, 190.1 second sentence, UPCA RoP, *supra* note 26.

207. *Id.*, Rules 191, 190.5.

208. *UPC Agreement*, *supra* note 16, Art. 32(1)(f).

209. *Id*.

210. An overview of the rights granted by the individual contracting states can be found in table III.A of the EPO brochure *National Law relating to the EPC*, *available at* https://www.epo.org/law-practice/legal-texts/national-law.html.

5. Corrective measures[211]

On request, the court may order appropriate measures with regard to products found to be infringing and, in appropriate cases, with regard to the materials or implements principally used in the creation or manufacture of those products. Such measures shall include (a) a declaration of infringement, (b) recalling the products from the channels of commerce, (c) depriving the product of its infringing property, (d) definitively removing the products from the channels of commerce, or (e) the destruction of the products or of the materials and implements concerned.[212] When considering such corrective measures, the court shall take into account the need for proportionality between the seriousness of the infringement and the remedies to be ordered, the willingness of the defendant to convert the materials into a noninfringing state, and the interests of third parties.[213] The court will order the defendant to carry out the measures at its own expense, unless particular reasons are invoked for not doing so.[214]

6. Publication of decision[215]

Finally, the court may order on request appropriate measures for the dissemination of information concerning the court's decision, including publishing the decision in full or in part in public media.

211. *UPC Agreement*, *supra* note 16, Art. 64.

212. *Id.*, Art. 64(2).

213. *Id.*, Art. 64(4).

214. *Id.*, Art. 64(3).

215. *Id.*, Art. 80.

7. Provisional and protective measures

Before or after the main proceedings on the merits have been started, the court may in case of a respective application also impose provisional and protective measures.[216] By way of summary proceedings, the court has to be satisfied with a sufficient degree of certainty that the applicant is the right holder and that the applicant's right is being infringed, or that such infringement is imminent.[217]

As provisional measures, the court may on request order preliminary injunctions;[218] the seizure or delivery of the goods suspected of infringing a patent right so as to prevent their entry into or movement within the channels of commerce;[219] a precautionary seizure of the movable and immovable property of the defendant, including the blocking of his bank accounts and other assets, if an applicant demonstrates circumstances likely to endanger the recovery of damages;[220] and an interim award of costs.[221] Also, the court may on request order preservation of relevant evidence, subject to the protection of confidential information, and the inspection of premises;[222] and may grant a freezing order that prohibits a party removing from its jurisdiction

216. *UPC Agreement*, *supra* note 16, Art. 62, and Rule 205 *et seq.*, UPCA RoP, *supra* note 26.

217. *UPC Agreement*, *supra* note 16, Art. 62(4).

218. *Id.*, Art. 62(1), and Rule 211.1(a), UPCA RoP, *supra* note 26.

219. *UPC Agreement*, *supra* note 16, Art. 62(3), and Rule 211.1(b), UPCA RoP, *supra* note 26.

220. *UPC Agreement*, *supra* note 16, Art. 62(3), and Rule 211.1(c), UPCA RoP, *supra* note 26.

221. *Id.*, Rule 211.1(d).

222. *UPC Agreement*, *supra* note 16, Art. 60, and Rule 192 *et seq.*, UPCA RoP, *supra* note 26.

any assets located therein or dealing in any assets, whether located within its jurisdiction or not.[223]

Preliminary injunctions will likely play a major role in the new system. The UPCA makes clear that a balancing of interests needs to be made in the course of deciding whether interim relief is granted. This is also the current national practice of the UPC member states.[224] However, many member states require that any interim relief is only granted in urgent cases. In Austria, its "urgency requirement" is applied broadly, making the local division in Vienna an interesting venue in cases where the patentee knows about the infringement for a relatively longer period of time (more than one to two months) and is still interested in obtaining a quick interim restraining order. The Hague also will play an important role when it comes to preliminary injunctions, since the Dutch courts have a reputation of entertaining requests for preliminary injunctions, even as a cross-border measure. The Munich local division also will be an attractive forum for bringing preliminary injunction requests, as the two national German judges of that division have a long track record with them.[225]

Should no infringement or threat of infringement be found subsequent to a revocation or lapse of the provisional measures, the court may order the applicant, on the defendant's request, to provide the defendant with appropriate compensation for any damage suffered as a result of those measures.[226]

---

223. *UPC Agreement*, *supra* note 16, Art. 61.

224. *Id.*, Art. 62(2).

225. *See, e.g.*, Phoenix Contact GmbH & Co. KG v HARTING Deutschland GmbH & Co. KG & Ors, C-44/21 (CJEU Jun. 3, 2022), https://curia.europa.eu/juris/liste.jsf?num=C-44/21&language=en.

226. *UPC Agreement*, *supra* note 16, Arts. 60(9), 61(2), 62(5).

C. Available defences for defendant

1. Introduction

Claims and actions under the exclusive competence of the UPC include "actions for actual or threatened infringements of patents and supplementary protection certificates and related defences, including counterclaims concerning licences."[227] Except for the explicitly mentioned "counterclaims concerning licences," it is left to interpretation what exactly qualifies as a "related defence" in an infringement action. Hence, and while the UPCA and UPCA Rules of Procedure set out some of the available defences, there is room to argue whether other defences might or might not be available to a defendant in an infringement action before the UPC. Undoubtedly, the UPCA is drafted with the intent to grant broad competence to the UPC where infringement actions are concerned, so that most defences known from patent infringement proceedings in participating EU member states should also be available in front of the UPC. There will be noticeable differences, however, some of which are highlighted in this Section.

2. Formal grounds for defence

a. Preliminary objection

As a first and formal ground for defence, the defendant may challenge the jurisdiction and competence of either the UPC or of the court's division, or of the language of the statement of claim. As to the jurisdiction and competence of the UPC, the competence of the national courts continues to apply for all actions that are not listed in Article 32 UPCA. In particular, the competency of national courts includes infringement actions for which the patent proprietor has declared an opt-out pursuant to

227. *Id.*, Art. 32(1)(a).

Article 83(3) UPCA. Chapter IV UCPA governs the competence of the local and regional divisions, depending on the place of infringement or defendant's domicile.[228] The required language of the statement of claim is governed by Rule 14 UPCA. If the defendant wants to raise the aforesaid defence, it is required to file a preliminary objection within one month of service of the statement of claim.[229] Importantly, for the UPC the question of *lis alibi pendens* seems to be considered as a matter of lack of competency,[230] so any related defence should be raised as part of such preliminary objection.

Importantly and as noted above,[231] timing is very critical, as an objection to the jurisdiction or competence of the UPC should be raised within one month after service of the complaint. Otherwise, jurisdiction and competence are irrevocably accepted.[232]

b. *Res judicata* defence

When raising a *res judicata* defence, the defendant informs the UPC that the subject of dispute has already been decided by a competent court. This applies, obviously, to earlier decisions by the UPC itself on the same subject matter. It also applies, however, to earlier decisions of national courts of participating EU member states, to the extent that they had jurisdiction over the subject of dispute. Therefore, if a national court has already ruled on the infringement of a national part of an EP patent by the same party, the UPC will be barred from again ruling on the infringement of such national part. Importantly, the UPCA does not seem to acknowledge preliminary and main procedures as

228. *Id.*, Art. 33.

229. Rules 19–21, UPCA ROP, *supra* note 26.

230. *UPC Agreement*, *supra* note 16, Art. 33(2).

231. *See supra* Section III.B (Case management of UPC litigation).

232. Rule 19(7), UPCA ROP, *supra* note 26, in conjunction with Rule 19(1).

relating to the same subject matter.[233] Arguably, the denial of a preliminary injunction by a court of an EU member state would therefore not preclude the UPC from granting an injunction effective in that same EU member state, should the patent-in-suit be moved under the UPC's jurisdiction. It appears unclear whether the acceptance of a preliminary injunction by the defendant as final and binding might make a difference in this regard. Procedurally, this defence provides for an absolute bar that can be raised at any time during the proceedings.[234]

c. Anti-suit and anti-anti-suit injunctions

Originally developed by common law courts, anti-suit injunctions (ASIs) are prohibitions on a party engaged in proceedings in a given court from bringing or continuing an action in a court of another state.[235] ASIs operate *in personam*, i.e., they are directed at the patentee in the foreign proceedings, not the foreign court. Technically speaking, an ASI has no extraterritorial effect. An ASI may, however, be a very powerful tool in the context of cross-border litigation in that it may be enforced indirectly, as noncompliance with the order may expose the litigant to severe penalties in the country where the injunction was issued.

Even though ASIs are usually not accepted in continental Europe with its civil law history, due to the fact that it raises issues of comity, so-called "anti-anti-suit-injunctions" (AASIs) have been accepted in order to bar a party to the proceedings

233. *See UPC Agreement*, *supra* note 16, Art. 62(5), Rule 213, UPCA ROP, *supra* note 26.

234. *Id.*, Rule 352.

235. David W Raack, *A History of Injunctions in England Before 1700*, 61 IND. L. J. 539, 545–56 (1986).

from pursuing an ASI in another forum.[236] The reason for allowing AASIs lies in the fact that the application for an ASI in another forum with the aim of preventing the enforcement of injunctive claims for patent infringement in the domestic market impairs the proprietary legal position of the right holder.

Whether the UPC will accept competence to issue such orders, be they ASIs or AASIs, largely depends on the judges' interpretation of Article 32(1)(c) UPCA ("actions for provisional and protective measures and injunctions"). The key question is whether this provision only covers provisional measures in view of a patent infringement or also ASIs and AASIs.

3. Noninfringement

Any patent infringement claim under the UPCA will either be based on Article 25 UPCA (right to prevent the direct use of the invention) or Article 26 (right to prevent the indirect use of the invention). Obviously, for such claims to succeed, the patentee will need to show that the defendant has used the invention, or that such use is imminent.[237] The defendant, on the other side, may show that no such use has occurred, either for a lack of any reserved act of use (such as making, offering, or placing on the market) in the relevant territory, or for the accused product or process not being covered by the scope of protection of the patent-in-suit. For the latter (and notwithstanding the burden of pleading and proof generally being upon the patentee),[238] the defendant may show that one or more features of the

236. *Cf.* Nokia v. Continental, Higher Regional Court Munich, decision of 12 Dec. 2019, docket-no. 6 U 5042/19; IPCom v. Lenovo, Tribunal de Grande Instance de Paris, decision of 8 Nov. 2019, docket.no. RG 19/59311; IPCom v. Lenovo, High Court of Justice (UK), [2019] EWHC 3030 (Pat).

237. *UPC Agreement*, *supra* note 16, Art. 62.

238. *Id.*, Art. 54.

asserted patent claims are not realized in the accused product or process.[239]

Article 27 UPCA provides for certain limitations on the effect of a patent, such as acts done privately and for noncommercial purposes, acts done for experimental purposes, or various other acts that are in the public interest or are exempted from patent protection by international treaties. If any of these situations apply, Article 27 provides for a corresponding (noninfringement) defence against any infringement claim.

4. Entitlement to use

The defendant may raise a defence concerning its entitlement to use the patented technology, which can be based on (a) the defendant's co-ownership of the patent, (b) a license that allows the defendant the use of the patent, or (c) the defendant's prior-use rights.

In regard to co-ownership of a patent, the UPCA and other regulations governing EP-UEs do not provide any specific rules that govern whether and to what extent a co-proprietor is entitled to make use of the patent. Arguably, this should be governed by the national law of the member state in which the property right has first come into existence. This would then lead to the application of German law, due to the EPO having its main offices in Munich.[240] Under German law, and in the absence to an agreement to the contrary, co-proprietors are subject to the law of tenancy in common. Under German case law, co-ownership of a patent usually comes with the entitlement of each co-proprietor to use the patented technology, subject to

239. As with most of the participating EU member states, features of a patent claim might be realized literally or under the doctrine of equivalents, *see supra* Section IV.A.4 (The doctrine of equivalents).

240. *See* TILMANN & PLASSMAN, *supra* note 63; *Unitary Patent Regulation*, *supra* note 17, at Art. 7.

certain "fair balance" restrictions and also possible financial obligations towards the other co-proprietor(s).[241]

As cited before, a "counterclaim concerning a license" is explicitly mentioned as a "related defence."[242] While the term counterclaim might be somewhat misleading, its use in the context of Article 32(1) UPCA leads commentators to conclude that it is not limited to counteractions (such as claims for a declaratory judgement on the existence of a license) but extends to the use as a defence argument against an infringement claim.[243] If a license exists, it provides for the patent proprietor's consent to use the patent, which would exclude the patent proprietor's right under the UCPA to prohibit the direct or indirect use of the invention.[244] Obviously, the scope of a license, which often comes together with various restrictions (e.g., on the permitted territory, on the duration of the use, or the subject matter of the use), can be subject to further dispute between the parties. In such cases, the wording in Article 32(1)(a) seems to imply that the UPC is in fact competent to also decide the interpretation of a contractual clause in a licensing agreement.

The prior-use right is acknowledged in Article 28 UPCA. Due to the "first to file" principle that applies in both the participating EU member states and for the EP-UE itself, the right secures the legitimate commercial interest of an earlier user of the invention, who failed to file first, to continue the use that existed at the priority date. Article 28 does not state any requirements, nor give any guidelines, as to the scope and application of this

241. For further details: *Gummielastische Masse II*, Bundesgerichtshof [BGH] [German Federal Supreme Court], GRUR Vol. 107, No. 8, 663–65 (2005).

242. *UPC Agreement*, *supra* note 16, Art. 32(1)(a).

243. TILMANN & PLASSMAN, *supra* note 63; *UPC Agreement*, *supra* note 16, Art. 32.

244. *Id.*, Arts. 25 & 26 UPCA (" . . . to prevent any third party not having the proprietor's consent . . .").

right in each situation. Instead, it refers to the rules of those participating EU member states in which the defendant would have enjoyed a prior use right if the patent were (hypothetically) asserted in the national courts. This mechanism is subject to criticism,[245] as it may lead to an EP-UE being enforceable in only some participating EU member states (namely those where no prior-use right would apply), which deviates from the otherwise unitary effect of the EP-UE.

5. Antitrust defences

While the UPCA does not set out any antitrust defences itself, it explicitly allows the application of EU law.[246] Thus, the restrictions on antitrust and anticompetitive behavior, as set out in Article 102 of the Treaty on the Functioning of the European Union,[247] are likely to apply in UPC courts, which are therefore expected to allow for corresponding defences.

In particular, it appears likely that the UPC will also apply the framework set out by the European Court of Justice in relation to anticompetitive behavior by the enforcement of standard essential patents (SEPs), including the necessity for an SEP holder to make a fair, reasonable, and nondiscriminatory (FRAND) offer and for an implementer to appropriately respond thereto.[248] Alternatively, or in addition, the UPC may also refer to the Intellectual Property Rights policies of the respective standard setting organizations and the SEP holder's contractual

245. TILMANN & PLASSMANN, *supra* note 63; *UPC Agreement*, *supra* note 16, Art. 28.

246. *Id.*, Art. 24(a).

247. Consolidated version of the Treaty on the Functioning of the European Union (Dec. 13, 2007), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.

248. Huawei Techs. Co. v. ZTE Corp., C-170/13 (E.C.J. 2015), https://curia.europa.eu/juris/liste.jsf?num=C-170/13.

obligations thereunder, which are to be interpreted according to national laws.[249] In the latter case, the choice of law of the respective Intellectual Property Rights policy might influence the scope of the available defence, which is considered as a possible concern.

It seems unclear whether the UPC will assume the task of setting a FRAND rate for a potential license on an SEP if the antitrust defence is raised, noting that courts of the participating EU member states have been reluctant, so far, to engage in such calculations themselves.

Importantly, the UPCA provides a suitable framework, including rules on confidential treatment, that allows for the disclosure of sensitive business information such as comparable license agreements, which are often used to determine whether a FRAND offer or FRAND counteroffer meet the applicable criteria.[250]

6. Exhaustion of rights

Article 29 UPCA limits the rights conferred by a European Patent (i.e., either an EP-UE or an EP that has become subject to the UPC's jurisdiction) to acts that are not subject to the principle of exhaustion, so that the exhaustion of rights is a direct defence also under the UPCA. Such exhaustion occurs if a product has been placed on the market in the EU by or with the consent of the patentee, which provides for an EU-wide (regional) exhaustion.

249. UPCA provides the UPC courts with the competence to also decide on these questions, as far as the national law of a participating EU member state is concerned. *See UPC Agreement*, *supra* note 16, Art. 24(1)(e).

250. *See id.*, Art. 59, and Rule 191, UPCA RoP, *supra* note 26.

7. Limitations and forfeiture

Article 72 UPCA sets out a five-year period after which actions "relating to all forms of financial compensation may not be brought." The way this provision is drafted ("may not be brought") indicates that the UPC needs to observe these time limits of its own motion,[251] so that this will not qualify as a defence in a stricter sense (i.e., something that needs to be actively raised by the defendant). Still, making the UPC aware of the relevant time periods and underlying facts will certainly be prudent for any defendant who wishes to benefit from Article 72. Secondly, while Article 72 extends to all forms of financial compensation, which includes all damages claims, it does not cover any nonfinancial claims, such as cease-and-desist claims. Five years after the last infringing act, however, any nonfinancial claim might be rendered moot (e.g., in the case of a cease-and-desist claim, due to the lack of repetition risk), so that a statutory limitation might be unnecessary.[252]

Forfeiture is not explicitly mentioned in the UPCA. However, according to Article 42(2), the UPC must apply all rules, procedures, and remedies provided for in the UPCA in a "fair and equitable manner," which may include the possibility to defend against a claim being brought extremely late (and against the justified expectations of the defendant), based on good-faith considerations. Also, Article 3(2) of the Enforcement Directive[253] and national laws of the participating EU member states, both of which need to be observed by the UPC,[254] contain similar

251. TILMANN & PLASSMANN, *supra* note 63; *UPC Agreement*, *supra* note 16, Art. 72.

252. TILMANN & PLASSMANN, *supra* note 63; *UPC Agreement*, *supra* note 16, Art. 72.

253. *Enforcement Directive*, *supra* note 188.

254. *UPC Agreement*, *supra* note 16, Art. 24(1).

concepts, so that a defence based on forfeiture is also likely to be available in front of the UPC.

8. Entitlement suits

Another possible defence is to claim ownership rights to the patent-in-suit. Such entitlement suits fall outside the jurisdiction of the UPC. They need to be filed with the competent national courts, most often at the place of domicile of the defendant. Such entitlement actions can have a very strong impact on the filing and prosecution strategy of proprietors, as Rule 14 EPC provides for an automatic stay of the prosecution in cases where an entitlement action has been filed before the grant of the EP.

While the UPCA does not explicitly acknowledge a related defence, Recast Brussels I and the UPCA Rules of Procedure should vest the UPC with the power to stay an infringement case pending the outcome of any such entitlement suit in a national court.[255] To what extent they may use such power will need to be developed by UPC case law.

9. Revocation counteractions

One of the most common defences against a claim for patent infringement is the challenging of the patent's validity. For the UPC system, there are two different options to challenge a patent that is being enforced in a pending infringement case: First, the defendant may file a separate revocation action with the competent division of the UPC,[256] or an opposition with the EPO, which then remains separate from the infringement case. Second, as an alternative or in addition to a separate nullity

255. Michael Nieder, *Vindikation europäischer Patente unter der Geltung der EPatVO*, GRUR, Vol. 117, 936–40 (2015) (analyzing *Recast Brussels I*, *supra* note 28, at Arts. 71(c) and 30(1) and Rule 295(k), UPCA RoP, *supra* note 26).

256. *UPC Agreement*, *supra* note 16, Art. 33.

action, the defendant may file a revocation counteraction, which will then be part of the infringement case and be dealt with simultaneously.

In a separate revocation action, the defendant will usually request a stay of the infringement case until a decision on the patent's validity, or that any decision on infringement is made subject to the condition that the patent subsequently is not held invalid. The UPC has discretion to grant these requests "if it is of the view that there is a high likelihood that the relevant claims of the patent will be held to be invalid on any ground by the final decision in the revocation proceedings or of the European Patent Office where such decision of the European Patent Office may be expected to be given rapidly."[257]

The revocation counteraction is governed by Rules 25–31 UPCA. While there might be some room to argue that the revocation counteraction might also be filed at any later point in time during the infringement proceedings (if sufficient justification is provided), Rule 9(2) UPCA foresees that any step, fact, evidence, or argument that has not been filed within a time limit set by the court or the Rules may be disregarded. In this regard, Rule 25(1) stipulates that the revocation action shall generally be filed together with the statement of defence already. It may contain all attacks against the patent's validity that would otherwise (or additionally) be included in a separate revocation action.

There will be numerous strategic considerations for a defendant in an infringement case at the UPC in deciding whether to file a separate revocation action, a revocation counteraction, or both. Some of these considerations include the question of which division may best decide on the patent's validity (a separate revocation action filed by a non-party to the infringement

257. Rule 118(2), UPCA RoP, *supra* note 26.

case can be brought to the central division), which division should handle the infringement case (a revocation counteraction creates the possibility of the UPC referring the entire case to the central division), the question of when relevant prior art will become available (late availability of such prior art may require a separate revocation action at that time, in order to avoid a possible exclusion for late filing), and whether the infringement case has been brought by the patent proprietor or a licensee (a revocation counteraction may require including the patent proprietor in the infringement case as a third party).[258] For a further discussion on these issues, please see Section D below.

D. Revocation actions

1. Grounds for revocation[259]

Regarding revocation grounds, Article 65 UPCA refers to Articles 138(1) and 139(2) of the European Patent Convention. Thus, the same grounds for revocation as in EPO opposition proceedings exist (including lack of novelty, lack of inventive step, lack of industrial applicability, noneligibility, insufficiency of disclosure, and added matter). Additionally, the revocation grounds (which to date can be relied on only in national revocation proceedings), namely an earlier unpublished national application, an extension of the scope of protection after grant, and lack of entitlement, are available.

Whereas it is clear that with respect to EP bundle patents, the invalidity ground of an earlier unpublished national application may only establish nullity of the national part of the EP bundle patent in the respective country, it is currently unclear what effect such a national unpublished elder right will have for

258. THOMAS BOPP & HOLGER KIRCHER, HANDBUCH EUROPÄISCHER PATENTPROZESS, (2019), at § 16.

259. *UPC Agreement*, *supra* note 16, Art. 65.

EP-UEs. The Unitary Patent Regulation[260] and the UPCA are silent in this respect, i.e., a transformation of an EP-UE into national parts of an EP bundle patent in those countries where the elder national right does not exist is not enacted.[261] As the unitary character of the EP-UE is one of the core elements of the Unitary Patent Regulation, it is highly doubtful whether the UPCA would find an EP-UE with respect to a specific national territory as partially invalid under Article 65(3) UPCA. However, it is up to the member state to open a route for late validation if an EP-UE is revoked due to an elder right that exists only outside the respective jurisdiction.[262] One feasible solution could be that an EP-UE is not revoked due to an elder national right at all, but the EP-UE is found not to be enforceable in the territory of the elder national right.[263] Such an approach was already found to be in line with the unitary character of EU trademarks.[264]

With respect to claims for lack of entitlement, Article 138(1) EPC only enacts revocation of an EP in cases where the owner has no right to the patent according to Article 60 EPC. However, the UPCA does not offer the option that an EP is transferred to

---

260. *Supra* note 17.

261. *See, e.g.*, Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (codification), Art. 139, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R1001.

262. Such late validations are currently provided for in at least Italy and Hungary; a draft legislation is under preparation in Austria.

263. *Cf.* Jan Ackerman/Horst Vissel, *Nationale ältere Rechte und europäische Patente mit einheitlicher Wirkung*, GRUR, Vol. 118, No. 7, 641–48 (2016).

264. Seydaland Vereinigte Agrarbetriebe GmbH & Co. KG v. BVVG Bodenverwertungs- und -verwaltungs GmbH, C-239/09 (CJEU Dec. 16, 2010), https://curia.europa.eu/juris/liste.jsf?language=en&num=C-239/09; DHL Express France SAS v. Chronopost SA, C-235/09 (E.C.J. Apr 12, 2011) at ¶ 45.

its rightful owner. Accordingly, if the rightful owner instead wishes a transfer of the EP, an action with the competent national court must be filed. Thus, in case of lack of entitlement, the rightful owner will be able to choose (also after the end of the transitional period) to file an action for revocation with the UPCA or an action for transfer with the competent national court.

2. Competence

Depending on whether (isolated) revocation proceedings are started or revocation is counterclaimed in pending proceedings, different divisions of the UPC are competent. Whereas actions for revocation of patents and for declaration of invalidity of Supplemental Protection Certificates[265] shall be brought before the central division,[266] a counterclaim for revocation in case of an action for infringement may be brought before the local or regional division in which proceedings are pending.[267] The concerned local or regional division will then have discretion (after having heard the parties) to proceed as follows: (a) proceed with infringement and counterclaim for revocation proceedings, whereas a technically qualified judge is added to the panel of three judges; (b) refer the counterclaim for revocation to the central division and suspend or proceed with an action for infringement; or (c) with the agreement of the parties, refer the case to the central division for decision.[268] In cases where revocation proceedings are pending, the patentee can choose either to file a counterclaim for infringement with the central division or to

265. *See supra* note 108.

266. *UPC Agreement*, *supra* note 16, Art. 33(4).

267. *Id.*, Art. 33(3).

268. *Id*.

lodge an infringement action before a regional or local division (see also Subsection 6 below).[269]

3. Relationship to EPO opposition proceedings

In the absence of any rules on priority between European Patent Office opposition proceedings and revocation actions before the UPC, both actions may run in parallel. The same is true for UPC proceedings and limitation proceedings before the EPO. However, the UPC may stay any action relating to a patent that is also the subject of opposition proceedings or limitation proceedings (including subsequent appeal proceedings) before the EPO where a decision in such proceedings may be expected to be given rapidly.[270] Additionally, the UPC may of its own motion or at the request of a party request the EPO to accelerate any opposition proceedings or limitation proceedings before it.[271]

4. Procedural steps

Revocation proceedings are initiated by lodging a statement of revocation at the Registry,[272] which shall contain details of the parties to the proceedings; an indication of the extent to which revocation of the patent is requested; one or more grounds for revocation supported by arguments of law; and, where appropriate, the claimant's proposed claim construction; an indication of the facts relied on, the evidence relied on, and an indication of any order which will be sought during the interim

269. *Id.*, Art. 33(5).

270. Rule 295, UPCA RoP, *supra* note 26.

271. *Id.*, Rule 298.

272. For description of the UPC Registry, *see supra* note 30.

procedure; and a list of documents, including witness statements, referred to in the statement for revocation.[273]

Revocation proceedings, like infringement proceedings, comprise a written procedure, an interim procedure, and an oral procedure.[274]

5. Strategic considerations for where to challenge validity of EP-UEs

Accordingly, the validity of EP-UEs may be attacked in three different fora: (i) the UPC central division by filing a revocation action; (ii) a UPC local or regional division by filing a counterclaim for revocation; and (iii) the EPO by filing an opposition.

Filing an opposition is only permitted within nine months of the publication of grant. Thus, in many disputes the defendant will not have the option to start opposition proceedings. However, if it is already known within the nine-month opposition term that a third party's patent may be critical, it may be advisable to start opposition proceedings.

The advantages of filing an EPO opposition may be summarized as follows:

- Lower costs
  - Official fees EPO: Opposition: € 840, Appeal € 2.785.
  - Official fees UPC: Revocation Action € 20.000; Appeal: € 20.000.
- Lower cost risk
  - EPO: Generally, each party bears its own costs.

273. Rule 44, UPCA ROP, *supra* note 26.

274. *See supra* Section III.B.

  - UPC: Costs are awarded to the winning party. The available costs that can be recovered depends on the (value) in dispute in the proceedings. E.g., a value of (or up to) € 250,000 results in (the minimum) award of € 38,000 in costs; and a disputed amount exceeding € 50 million results in (the maximum) award of € 2 million in costs.

- Larger territorial effect
  - EPO opposition covers the EP patent as whole (EP-UE, national validations, and non-EU member states, e.g., United Kingdom, Switzerland).
  - UPC proceedings have legal effect only in the participating member state (currently 17 UPCA-member states as opposed to 38 EPC-member states).

- Nondisclosure of the opponent's identity
  - EPO: Oppositions filed by a strawman (i.e., proxy) are generally allowed, unless there is an abuse of law, e.g., the opposition is filed in the interest of the proprietor itself.[275]
  - UPC: Anybody who is concerned by a patent may bring actions in accordance with the Rules of Procedure.[276] Thus, it seems rather likely that some legal or economic

275. G9/93, Opposition by patent proprietor, European Patent Office, Enlarged Board of Appeal, (July 6, 1994), https://www.epo.org/law-practice/case-law-appeals/recent/g930009ep1.html.

276. *UPC Agreement*, *supra* note 16, Art. 47(6).

interest must be proven and that a straw-man as the claimant will not be allowed.

The advantages of filing a revocation action or counterclaim for revocation with the UPC may be summarized as follows:

- No time limitation
  - EPO: Opposition term limited to nine months after publication of grant.
  - UPC: No time limit.
- Shorter duration
  - EPO: Aims for first-instance decision within 24 months, currently.
  - UPC: Aims for first-instance decision within 12 months.
- Further revocation grounds:
  - UPC: Same revocation grounds as at EPO plus lack of entitlement, extension of scope of protections after grant, and national elder right.

As there is no rule that excludes parallel opposition proceedings before the EPO and revocation proceedings before the UPC, there may be scenarios in which both proceedings are initiated. Parallel proceedings may be initiated if it is an extremely important case and the costs are acceptable to the proprietor. There may also be situations in which the defendant or the proprietor is barred from introducing further prior art documents in the pending proceedings. As the time limits are much stricter in UPC proceedings, the proprietor may be pushed to disclose its arguments and claim amendments much earlier if revocation proceedings are initiated in addition to opposition proceedings.

6. Counterclaims for infringement / separate actions for infringement

The defendant should keep in mind that filing a standalone revocation action (i.e., a revocation action not in response to a corresponding infringement action) may trigger either a counterclaim for infringement[277] or a standalone action for infringement brought before a local or regional division.[278]

E. Amending the patent-in-suit before the UPC

1. Introduction

Patent amendments are often necessary in order to establish a defence position during patent revocation proceedings, where patent proprietors may expect the opposing party to perform an in-depth analysis of the validity of the relevant set of claims asserted. Accordingly, an EP-UE or traditional non-opted-out EP may be amended before the UPC as a defence to a counterclaim for revocation[279] or as a defence in a revocation action.[280] The proprietor may amend both the claims or the specification and may, where applicable and appropriate, include one or more alternative sets of claims (i.e., auxiliary requests).

2. Amendments and requirements

Amendments must comply with Articles 84 and 123(2)-(3) EPC and result in a valid set of claims that are clear.[281] They must not introduce subject matter that extends beyond the

277. Rule 49(2)(b), UPCA ROP, *supra* note 26.

278. *UPC Agreement*, *supra* note 16, Art. 33(5); *see also supra* Section III.D.2 (Counterclaim for infringement following a claim for revocation).

279. Rule 30, UPCA ROP, *supra* note 26.

280. *Id.*, Rule 49.

281. *Id.*, Rule 30.1(b).

content of the application as filed or extends the protection conferred by the patent. Amendments must be accompanied by an explanation as to why the claims are valid and how the EPC requirements are satisfied. In this respect, the UPC will likely rely on case law from the Boards of Appeal of the EPO, though this is not specified in the UPCA or the Rules of Procedure. If relevant, amendments shall also be accompanied by an explanation as to why the claims are infringed.[282]

Amendments may be both conditional and unconditional, meaning that they may be proposed as auxiliary requests to be assessed only if a higher-ranking request is rejected by the UPC. However, if the proposed amendments are conditional, the proposals, i.e., the number of auxiliary requests, must be reasonable under the circumstances of the case.[283]

It will be interesting to learn how the UPC will interpret what number of auxiliary requests constitutes "reasonable." It is expected that the UPC will apply a rather strict approach to this question.

3. Language

Any proposed amendments must be filed in the language in which the patent was granted. If the language of the proceedings at the UPC is not the language in which the patent was granted, the proprietor must also provide a translation of the proposed amendments in the language of the proceedings. If the patent is an EP-UE, the proprietor must also, if requested by the defendant, provide a translation of the proposed amendments in either the language of the defendant's domicile in a member state of the EU, or in the language of the place of the alleged

282. *Id*.

283. *Id.*, Rule 30.1(c).

infringement or threatened infringement in a contracting member state.[284]

4. The effect of granted amendments

Amendments of EP-UEs granted by the court shall have effect in all the participating member states.[285] In the case of an EP, the decisions of the UPC shall cover the territory of those UPC contracting member states for which the EP has effect.[286]

5. When to file proposed amendments

Importantly, the proposed amendments should be filed with the statement of defence to the revocation or the counterclaim for revocation action, as requests for amendments filed subsequently may only be admitted into the proceedings with the permission of the court.[287] It is expected that the UPC will apply this rule rather strictly, highlighting the need for speedy case management and analysis.

6. Risks

The requirement for filing the request to amend the patent when lodging the statement of defence to the revocation or the counterclaim for revocation action poses a major risk to proprietors who may be under time pressure when confronting a revocation action. Thus, patent proprietors are advised to perform an analysis of potential weaknesses in their patent claims as early as possible and to carefully consider the possibilities of amending the patent before the UPC even prior to being confronted with a counterclaim for revocation.

---

284. *Id.*, Rule 30.1(a).

285. *Unitary Patent Regulation, supra* note 17, Art. 3.2.

286. *UPC Agreement*, *supra* note 16, Art. 34.

287. Rule 30.2, UPCA ROP, *supra* note 26.

Further, patent proprietors should be cautious in proposing unconditional amendments, as it may endanger the patent if the UPC considers the amendments not to comply with the requirements of Rule 30.1(b) UPCA.

Proprietors of EPs that do not benefit from unitary effect (e.g., patents having different sets of claims for different participating member states) should also note that it seems unclear from Article 34 UPCA whether different sets of claims can survive amendments before the UPC.

F. Declaration of noninfringement actions (DNI) before the UPC

1. Requirements

An action for declaration of noninfringement (DNI)—i.e., a request that the performance of a specific act does not, or a proposed act would not, constitute an infringement of a patent—may be lodged by the person who acts or plans to act against the patentee or a licensee, if the patentee or licensee has asserted that the act is an infringement.[288] The conditions for such an assertion are nonexhaustively specified in Rule 61(1) UPCA. It remains to be seen whether further conditions will be specified by the case law.[289] The requirements set out in Rule 61(1) are as follows: "An allegation of the patentee that the act concerned constitutes an infringement, *or*, in the absence of such allegation, a written request by the person contemplating the act concerned for a written confirmation of non-infringement and receipt of such confirmation within one month."

288. *Id.*, Rule 61.

289. TILMANN & PLASSMANN, *supra* note 63; *UPC Agreement*, *supra* note 16, Art. 32.

What will eventually constitute an "assertion" is not clearly defined in Rule 61(1).[290] However, if the patentee or licensee requests submissions of a cease-and-desist declaration, this will undoubtedly qualify as an assertion.[291]

The DNI action shall be directed (only) against the patentee or licensee who has asserted an infringement or refused or failed to give acknowledgment of noninfringement after receiving a written request.[292] Thus, if the licensee asked for a cease-and-desist declaration, the DNI action can be directed only against the licensee.[293] To direct a DNI action against the patentee as well, it will be necessary to request a noninfringement declaration separately from the patentee and for the patentee to have refused or failed to give such an acknowledgment.

Accordingly, the UPCA Rules of Procedure explicitly refer to two alternatives (infringement assertion by the patentee or licensee, and failure or refusal to acknowledge noninfringement by the patentee or licensee) in which a DNI action will be allowed.

However, the UPCA generally states that any natural or legal person who is concerned by a patent may bring actions, i.e., anyone who has a legitimate interest deserving protection.[294] Thus, there may be other scenarios in which the claimant may also successfully argue that it is concerned by a specific patent, and therefore, the requirements for a DNI action, namely a legitimate interest,[295] may be met. For example, if the patentee

290. *Id.*

291. *See* Rule 61, UPCA ROP, *supra* note 26.

292. *Id.*, Rule 61(2).

293. *Id*.

294. *UPC Agreement*, *supra* note 16, Art. 47(6).

295. TILMANN & PLASSMANN, *supra* note 63; *UPC Agreement*, *supra* note 16, Art. 32.

asserts that an act by the DNI applicant's customer amounts to an infringement, the fact that the customer might have a claim for indemnification against the DNI applicant might suffice to show legitimate interest.[296]

Another scenario could be a so-called FRAND undertaking[297] to a standardisation organization according to which a specific patent is declared to be standard-essential, i.e., that its technical teaching is necessary to make use of a specific standard. In this case, anybody implementing the standardized technology is potentially affected by this patent and would therefore have a legal basis for lodging a DNI action.[298]

2. Competence—Interaction with infringement actions

DNI actions must be lodged with the central division of the court.[299] However, there are two exceptions to this general rule: an infringement action already pending before the regional or local division, or the parties agreeing to bring the DNI action before any other division of the court. Thus, if an infringement action is already pending before a local or regional division, this division is also competent for a DNI action.[300]

If an infringement action is already pending, a DNI action is only admissible under specific circumstances: the action should be admissible when a limitation of the patent in dispute or a right to use or exhaustion of the patent in dispute is asserted.

296. *Cf.* for Germany: Higher Regional Court Munich, decision of 12 May 2005, docket-no. 29 U 4733/04.

297. If a patent is declared essential to a standard as set by a standardization organization, the patentee usually submits an undertaking to be willing to license the patent concerned on FRAND-terms (i.e., on a fair, reasonable and non-discriminatory basis).

298. TILMANN & PLASSMANN, *supra* note 63, at 1616.

299. *UPC Agreement*, *supra* note 16, Art. 33(4).

300. *Id.*, Art. 32(1)(b).

However, if the DNI action is based only on the assertion that the acts conducted do not fall under the scope of protection or no infringing acts were conducted,[301] such a DNI action would be inadmissible, as these assertions will already lead to a rejection of the infringement action, and thus there is no legitimate interest in such a DNI action.[302]

If a DNI action is pending before the central division prior to an infringement action being lodged, the DNI action shall be stayed if the infringement action between the same parties or between the holder of an exclusive license and the party requesting a DNI relating to the same patent is brought before a local or regional division within three months of the date on which the DNI action was initiated before the central division.[303] Accordingly, the defendant cannot draw the dispute from a competent local or regional division of the patentee's choice if the patentee files an infringement action within three months from the defendant's initiation of a DNI action. If an infringement action is filed after the three-month-term, there's no mandatory stay of DNI actions as stipulated in Article 33(6) UPCA. However, in case of such a "late-filed" infringement action, the presiding judges of the central division and the local or regional division concerned shall consult to agree on the future progress of proceedings, including the possibility of a stay of one action.[304]

301. *Id.*, Arts. 25–26.

302. TILMANN & PLASSMANN, *supra* note 63, at 654.

303. *UPC Agreement*, *supra* note 16, Art. 33(6).

304. Rule 76(3), UPCA ROP, *supra* note 26.

3. Procedural steps[305]

DNI proceedings are initiated by lodging a statement for declaration of noninfringement at the Registry.[306] The statement shall contain the same details as in revocation or infringement proceedings. In addition, particulars are to be included to confirm that the claimant has a legal interest in lodging the action.[307]

The written procedure in DNI proceedings basically corresponds to the procedure in infringement proceedings. Accordingly, a defence is to be filed within two months, and optionally, a reply to the defence and a rejoinder to the reply are to be filed within one month. As in infringement proceedings, the written procedure is followed by an interim procedure and an oral procedure.

A fixed court fee of € 11,000 is to be paid.[308] If the value of the dispute exceeds € 500,000, a value-based fee is paid in addition to the fixed fee. The value of an action for a DNI is calculated as for an infringement action.[309]

4. Strategic considerations

By filing an admissible DNI action with the UPC (under the conditions set out above), a defendant may block the patentee during the transitional period from starting national infringement actions.[310] However, the claimant cannot block the

305. *Id.*, Rule 63 *et seq*.

306. For description of the UPC Registry, *see supra* note 30.

307. *Cf.* requirements set forth in Rule 61, UPCA RoP, *supra* note 26.

308. *See* Unified Patent Court Administrative Committee, Table of Court Fees (July 8, 2022), https://www.unified-patent-court.org/sites/default/files/upc_documents/ac_05_08072022_table_of_court_fees_en_final_for_–publication_clean.pdf.

309. *See id*.

310. *Recast Brussels I*, *supra* note 28, Art. 29.

patentee or licensee from filing an infringement action with the UPC. On the contrary, as the DNI action is only mandatorily stayed if the patentee or licensee files the infringement action within three months from the date the DNI was lodged, the DNI action may trigger or at least motivate the patentee or licensee to start an infringement action within the three-month term.

G. Evidence proceedings before the UPC

1. Rules governing evidence

The system adopted in the UPC system is based on continental law tradition where:

- The burden of the proof lies on the parties relying on specific facts.[311]
- No discovery-like or disclosure-like procedures are provided.
- The statement of claim should present all evidence of the allegations it contains and include the motions requested that will be sought during the written phase of the procedure.
- Should a fact be not contested by a party, it is considered as true between the parties.[312]
- But the court can order a party to submit the evidence of an alleged fact if this evidence is under the control of that party. The failure to provide such evidence should be taken into consideration by the court in its decision.[313]
- Among the means of evidence available in front of the UPC, the Rules of Procedure give the

311. *UPC Agreement*, *supra* note 16, and Rule 171.1 UCPA.

312. Rule 171.2, UPCA ROP, *supra* note 26.

313. *Id.*, Rule 172.2.

> following nonexhaustive list: written evidence (in particular, documents, written witness statements, plans, drawings, photographs), expert reports and reports on experiments carried out for the purpose of the proceedings, physical objects (in particular devices, products, embodiments, exhibits, models), electronic files, and audio/video recordings.[314]

The UPC system provides a list of means to help the claimant to bring evidence of its allegation, including a hearing of the parties, requests for information, production of documents, hearing of witnesses, opinion by experts, inspection, comparative tests or experiments, and affidavits.[315]

One of the most interesting means is the possibility to obtain an order to preserve evidence, otherwise named "*saisie*," by reference to (but not identical to) the famous French *saisie-contrefaçon*.[316]

2. Reversal of the burden of proof

The UPCA provides the possibility of reversal of the burden of proof in the specific case where the subject matter of the patent is a process for obtaining a new product or when there is substantial likelihood that the identical product was made by the patented process and the patentee, despite reasonable efforts, has been unable to bring evidence thereof.[317] This reversal of the burden of proof is already widely in place in national European legislations.

---

314. *Id.*, Rule 170.

315. *UPC Agreement*, *supra* note 16, Art. 53.

316. For discussion of *saisie* before the UPC, *see infra* Section IV.G.4.d (Orders to preserve evidence (*saisie*) and orders for inspection).

317. *UPC Agreement*, *supra* note 16, Art. 55.

3. Confidentiality measures

As a matter of principle, all proceedings pending in front of the UPC are deemed to be public. Court rooms are open to the public, and documents of the proceedings filed in the UPC Registry[318] are available. Nevertheless, both the UPCA and the Rules of Procedure refer to the protection of confidential information of a party, of a third party, or even in the general interest of justice or public order,[319] which may lead to closing the doors of the court or to limiting disclosure of the documents (or content thereof) available from the Registry.[320]

In the context of gathering evidence, the Rules of Procedure require the court to take into account the legitimate protection of confidential information. This applies to requests to produce evidence,[321] to preserve evidence,[322] and for inspection,[323] where only named persons subject to appropriate terms of nondisclosure can have access to the evidence produced if it contains confidential information.

The same protection applies with respect to a professional privilege or a duty of confidentiality imposed by national legislation, such as attorneys' privilege[324] or confidentiality imposed on spouse, descendant, sibling, or parents who cannot be heard as witness if it exposes them to criminal prosecution under the relevant national law.

---

318. For description of the UPC Registry, *see supra* note 30.

319. *UPC Agreement*, *supra* note 16, Art. 45.

320. Rule 262, UPCA RoP, *supra* note 26.

321. *Id.*, Rule 190.

322. *Id.*, Rule 196.

323. *Id.*, Rule 199.

324. *Id.*, Rule 287.

4. Obtaining and gathering evidence

In order to help the claimant in its task, the UPCA and the Rules of Procedure provide various means to obtain and gather evidence, including witness and expert statements, orders to produce evidence and to communicate information, orders to preserve evidence, and orders for inspections. An overview of these means is provided below.

a. Witnesses and experts of the parties[325]

Witness statements can be made in writing or orally, the latter being available only if a written statement is contested by the adverse party and if an application is filed for the hearing of a witness in person. The refusal by a witness to be heard by the court can be sanctioned by a fine.[326]

An exception to the signing of a witness statement or the hearing of a witness can be raised if this witness is a spouse (or partner equal to a spouse according to the relevant national law), descendant, sibling, or parent of a party. The same exception applies if the witness is subject to professional privilege or other duty of confidentiality or if the testimony exposes the witness to criminal prosecution.[327]

The Rules of Procedure require that the witness confirms the obligation to tell the truth and the witness's liability in case of a breach of this obligation. The hearing of a witness can be done through videoconferencing.[328]

One important element that differentiates the UPC system from the common law system is that witnesses can be

325. *Id.*, Rules 175–81.

326. *Id.*, Rule 179.

327. *Id.*, Rule 179.3.

328. *Id.*, Rule 178.6.

questioned only by the judge or by the parties under the control of the judge. There is no cross-examination of witnesses in the sole hands of the parties.[329]

Experts can be appointed by the parties to provide expert evidence and assist the court impartially on matters relevant to the witness's area of expertise.[330] The Rules of Procedure state that this duty overrides "any duty to the party pertaining him/her" and that the expert should not "act as an advocate for any party to the proceedings," although in practice, parties will necessarily have experts' statements supporting their positions in court.

Experts can conduct experiments upon reasoned request from a party or the court[331] in order to prove a fact for the purpose of the proceedings.

b. Court experts[332]

As an exception to the principle that the parties should prove the facts they allege, the UPCA and Rules of Procedure provide the possibility for the parties to ask the court for the appointment of an expert. An indicative list of experts is established and managed by the registrar of the court, but parties can also make suggestions. The same rules of impartiality and absence of conflict of interest that apply to judges also apply to court-appointed experts.[333]

The court order appointing an expert details the questions asked to the expert and the timing of the reply. The order can be

329. *Id.*, Rules 177.2, 178.4, and 178.5.

330. *Id.*, Rule 181.

331. *Id.*, Rule 201.

332. *Id.*, Rules 185–88.

333. *UPC Agreement*, *supra* note 16, Art. 57.

appealed only upon authorization of the court[334] or with the judgement on the merits.

c. Orders to produce evidence[335]

The UPCA and Rules of Procedure[336] provide for the possibility to obtain evidence from an adverse party or a third party. The claim for production of evidence should contain reasonably available and plausible evidence in support of the claim and substantiate "specified evidence" that lies in the control of the adverse or third party. This measure cannot be used as a fishing expedition.

The judge-rapporteur can give the adverse party the opportunity to oppose a claim for production of evidence and should in any case take into consideration the interest of that third party when granting the order. Failure to comply with the order to produce evidence can be taken into consideration when deciding on the issue in question.[337] Protection of confidential information is also taken into account and may lead to a limitation of the number of people having access to the evidence, along with an obligation of nondisclosure.[338]

334. Rule 220.2, UPCA ROP, *supra* note 26.

335. *UPC Agreement*, *supra* note 16, Art. 59(1), and Rule 190, UPCA ROP, *supra* note 26.

336. *Id.*, Rule 190.

337. *Id.*, Rule 190.6.

338. *Id.*, Rule 190.1.

d. Orders to preserve evidence (*saisie*) and orders for inspection[339]

The order to preserve evidence, specifically referred to as "*saisie*," may become one of the most used measures to gather evidence in front of the UPC should it be used as often as it is in French proceedings. A few elements are nonetheless different from the French *saisie*, as detailed below.

An order to preserve evidence can be requested to obtain a detailed description with or without the taking of samples, the physical seizure of allegedly infringing goods, the physical seizure of the materials and implements used in the production or distribution of those goods, and any related documents and digital media and data (including passwords necessary to access them).[340] An application can be filed by any party entitled to launch patent infringement proceedings against the defendant before or in the course of patent infringement proceedings.

One major deviation from the French-type *saisie* is that the defendant can be heard by the court when such application is filed, even if the application was filed ex parte by the applicant. In such case, when the judge-rapporteur informs the applicant that it intends to hear the defendant, the rules of procedure offer to the applicant the possibility to withdraw the application (in such case, the application does not appear in the Registry[341]).[342]

The applicant must justify the filing of the grant of an ex parte order, in particular due to urgency or demonstrable risk of destruction or unavailability of evidence.[343] To obtain the

339. *UPC Agreement*, *supra* note 16, Art. 60, and Rules 192–99, UPCA ROP, *supra* note 26.

340. *Id.*, Rule 196.

341. For description of the UPC Registry, *see supra* note 30.

342. Rule 194.5, UPCA ROP, *supra* note 26.

343. *Id.*, Rule 197.

order, the applicant must also state why the requested measures are needed to preserve evidence and, if the application is filed before the launch of proceedings on the merits, a concise explanation of the action that will be started before the court.[344]

As with the French *saisie*, the Rules of Procedure impose a sort of duty of loyalty on the applicant, who must disclose any material fact it knows that might influence the court when deciding whether to grant the order. The protection of confidential information is also taken into account by the court, and the order may limit the disclosure of the information to certain people subject to appropriate terms of nondisclosure.[345]

One way to force the applicant to withdraw its application or to obtain from the court the opportunity to contest the application is to file a protective letter.[346] Inspired from the German practice of "*Schutzschrift*," any party who considers it likely that a measure will be taken against it can file a protective letter with the Registry. The party may, through its protective letter, challenge any facts that may likely be presented against it and also may challenge the validity of the patent(s) in question. Once received by the Registrar, the protective letter is shared by the Registry with all divisions of the court and should remain available for six months (with the possibility of extension of six additional months). Should the other party take a measure against the defendant who filed the protective letter, the protective letter is then sent by the Registry to the division where the application for measures has been filed and to the applicant seeking such measures.

If a preservation order is granted before the launch of any patent infringement proceedings on the merits, the applicant

344. *Id.*, Rule 192.

345. *Id.*, Rule 196.

346. *Id.*, Rule 207.

shall launch such proceedings within 31 calendar days or 20 working days from the day specified in the order.[347] Otherwise, the defendant can ask for a revocation of the order.

The court's ruling can be appealed within 15 days by either the applicant (if the order has been rejected) or the defendant.[348] The defendant may ask for a review of the order within thirty days after the execution of the preservation order to have the order revoked or amended.[349]

The UPCA and the Rules of Procedure also give the possibility to obtain an order allowing for inspection[350] of products, devices, methods, premises, or local situation in situ. The same rules apply to the order to preserve evidence.

e. Other evidence

The UPCA and the Rules of Procedure permit one party to obtain an order to freeze assets[351] in order to prevent another party from removing assets from the jurisdiction of the court or dealing in any assets, whether located within its jurisdiction or not.

The UPCA also provides for letters rogatory to obtain production of documents or the hearing of witnesses or experts by other competent courts or authorities outside of the EU.[352] For

347. *Id.*, Rule 198.

348. *UPC Agreement*, *supra* note 16, Art. 73.

349. Rule 197, UPCA RoP, *supra* note 26.

350. *UPC Agreement*, *supra* note 16, Art. 60, and Rule 199, UPCA RoP, *supra* note 26.

351. *UPC Agreement*, *supra* note 16, Art. 61, and Rule 200, UPCA RoP, *supra* note 26.

352. *Id.*, Rule 202.

the same request within the EU, Recast Regulation No. 2020/1783 applies.[353]

5. Interplay with national systems

Article 32 UPCA, which relates to the exclusive competence of the UPC, does not refer to measures relating to evidence. It may therefore allow for evidentiary procedures stemming from the national legislation of a contracting member state.

One can therefore imagine using the French-type *saisie*, which will only be granted ex parte, to obtain evidence within the French territory prior to launching a patent infringement proceeding in front of the UPC.

H. Procedures for the determination of damages and compensation before the UPC

Although damages can be requested at the same time as the procedure determining liability,[354] the Rules of Procedure also mention the possibility to have damages determined through separate proceedings.[355] Article 68 UPCA states that the injured party in patent infringement proceedings is entitled to obtain damages in relation to the "harm actually suffered" as a result of the infringement.

Typical of the European continental law system, the UPCA does not allow punitive damages. Article 68.3 UPCA mirrors Article 13.1 Enforcement Directive[356] as to the elements to be

353. Regulation (EU) 2020/1783 of the European Parliament and of the Council of 25 Nov. 2020 on cooperation between the courts of the Member States in taking of evidence in civil and commercial matters (taking of evidence) (recast), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R1783&from=EN; *see also* Rule 173, UPCA ROP, *supra* note 26.

354. *Id.*, Rule 118.

355. *Id.*, Rule 125.

356. *Enforcement Directive*, *supra* note 188.

taken into consideration by the court to set the damages. It refers to negative economic consequences, which includes lost profits, unfair profits made by the defendant, and where appropriate, moral damages. It also contains the option of ordering a lump sum payment equal to or greater than the amount of royalties or fees that would have been due had the defendant requested permission.

Interestingly, the UPCA provides the possibility to lower damages in cases where the defendant did not "knowingly, or with reasonable grounds to know" engage in the infringing activity. In such case, the court has the option of ordering only the recovery of profits or the payment of compensation.[357]

As to the actual damages proceedings, the Rules of Procedure indicate that such proceedings should be initiated no later than one year from the service of the final decision on the merits (including appeal) on both validity and infringement. Damages can also be requested in case of a revocation of an order to preserve evidence,[358] revocation of provisional measures,[359] or noncompliance with an order of the court.[360]

The application for the determination of damages must indicate all redress and interests asked, all supporting facts and evidence, and may contain an application for the laying of open books. This application is registered and served upon the defendant, who has two months to file a defence. The patentee is given a month to reply to the defence, and the defendant can file a rejoinder within a month from receiving the reply. Specific timing applies for the request to lay open books.[361] If the request

357. *UPC Agreement*, *supra* note 16, Art. 68.4.

358. Rule 198.2, UPCA ROP, *supra* note 26.

359. *Id.*, Rule 213.2.

360. *Id.*, Rule 354.4.

361. *Id.*, Rules 141–42.

is granted, the court orders the defendant to lay open books and sets the time period within which the procedure for the award of damages shall be continued.[362]

If the court varies or revokes a decision or order, a party that was injured by the enforcement of the original decision or order may move for appropriate compensation.[363]

It will be interesting to see the approach that will be taken by the UPC in terms of setting damages. Jurisdictions within the European Union differ on this aspect, with some countries allowing high amounts for damages and others allowing low (or even no) damages.

I. Cost awards before the UPC

As a general rule and unless equity requires otherwise, the unsuccessful party shall bear the reasonable and proportionate legal costs and other expenses incurred by the successful party, up to a ceiling set in accordance with the Rules of Procedure.[364] The court may award costs differently where a party only succeeds in part and in exceptional circumstances. Unnecessary costs shall always be borne by the party causing such costs. The court may order a party to provide adequate security for legal costs incurred by the other party.

The court shall decide in principle on the obligation to bear legal costs and may order an interim award of costs in the decision on the merits.[365]

Cost decisions are made by the judge-rapporteur in accordance with the procedure laid down in Chapter 5 of the Rules of Procedure. The successful party must seek a cost decision

362. *Id.*, Rule 144.

363. Rule 354.2, UPCA ROP, *supra* note 26.

364. *UPC Agreement*, *supra* note 16, Art. 69.

365. Rules 118(5) & 150(2), UPCA ROP, *supra* note 26.

within one month of service of the decision on the merits and may recover court fees, attorney fees, costs for experts and witnesses, and other expenses. The judge-rapporteur may require the applicant to provide written evidence of all costs and shall allow the other party to respond.

The standing judge of the court of appeal decides on granting leave to appeal and appeals of cost decisions.[366]

Although Article 69 UPCA stipulates that a ceiling shall apply for legal costs and expenses, the UPCA Rules of Procedure instruct the Administrative Committee to adopt ceilings only with respect to representation costs.[367] According to the draft scale of recoverable cost ceilings, the ceilings for representation costs are based on the value of the proceedings and range from € 38,000 up to a maximum of € 2 million if the value of the proceedings exceeds € 50 million.[368]

J. Provisional and protective measures

The court may grant provisional injunctions to prevent any imminent infringement or to prohibit, or make subject to the lodging of a guarantee, the continuation of an alleged infringement.[369] The court may make a prohibitory injunction subject to a recurring penalty payment.

The court may also order seizure or delivery up of allegedly infringing products and, if the applicant demonstrates circumstances likely to endanger the recovery of damages, precautionary seizure of the defendant's property.

The court may require the applicant to furnish evidence to demonstrate with a reasonable degree of certainty that the

366. *Id.*, Rule 221.

367. *Id.*, Rule 152(2).

368. *Id*.

369. *UPC Agreement*, *supra* note 16, Art. 62.

patent is valid and infringed. The court may weigh up the interests of the parties prior to granting or refusing injunctions, and the court shall have regard to any unreasonable delay in seeking the provisional measures.[370] Neither the UPCA nor the Rules of Procedure clarify whether the court will apply a presumption of validity or what is required to rebut such presumption.

The court may invite the defendant to object to the application for provisional measures, and it may hold an oral hearing to which it may summon either both parties or only the applicant. In exercising its discretion regarding the procedure, the court shall take into account whether the EPO has upheld the patent in opposition proceedings, the urgency of the action, the reasons for any ex parte measures requested, and any protective letter filed by the defendant.

If necessary, and particularly where delay is likely to cause irreparable harm, the court shall order provisional and protective measures without hearing the defendant. If the court grants ex parte measures, the defendant shall be notified and the court shall review the measures within reasonable time. If the court refuses ex parte measures, the claimant may withdraw the application and request that it remains confidential. To mitigate the risk of ex parte measures, any person entitled to start proceedings under Article 47 UPCA may file a protective letter. A protective letter is valid for an extendable period of six months and shall be forwarded to the panel or judge appointed to decide on provisional measures in relation to the patent covered by the protective letter.

A patentee may lodge an action for provisional measures before or after starting main proceedings on the merits. In the former case, the patentee must bring an action leading to a decision on the merits within the longer of 31 calendar days or 20

370. Rule 211, UPCA RoP, *supra* note 26.

working days, or the court shall revoke any measures ordered upon the request of the defendant.

If the court revokes the measures or if the court subsequently finds that the patent was not infringed, the defendant may ask the court to order the patentee to provide appropriate compensation for any damage suffered. As a condition for granting the measures, the court may require the patentee to lodge adequate security to ensure such compensation.

The court's orders to grant provisional and protective measures take immediate effect. Parties may appeal to the court of appeal. Leave to appeal is not required. An appeal will not suspend the effect of the order, but the court of appeal has the power to suspend the effect upon request by the appellant.

V. ENFORCING A JUDGEMENT OF THE UPC UNDER THE NATIONAL PROCEDURAL RULES

A. Requirements for enforcing a UPC judgement

1. Starting point: Recast Brussels I

Principally, decisions by a court of an EU member state are enforceable in all EU member states subject to the requirements stipulated in Chapter III of Recast Brussels I.[371] However, Recast Brussels I is not applicable to decisions of so-called common courts—like the courts established under the UPC-regime[372]—if enforcement is sought in an EU member state over which the particular common court has jurisdiction. Accordingly, if a decision of a local or regional division of the UPC is sought to be enforced in an EU member state that is a party to the UPCA, the rules of the UPCA supersede the rules of Recast Brussels I.[373] Chapter III of Recast Brussels I remains only applicable for cases where a judgement of a local or regional division of the UPC is sought to be enforced in an EU member state that is not party to the UPCA.[374] During the transitional period, the enforcement remains to be governed by Recast Brussels I in cases of either an opt-out or an action brought before national courts.[375]

2. Enforcement under the UPCA regime

The remedies that can be sought by the claimant are permanent injunctive relief[376] (in particular, cease-and-desist orders), removal from the distribution channels, recall and

371. *Recast Brussels I*, *supra* note 28.

372. *Id.*, Art. 71a (2).

373. *See id.*, Art. 71d (2).

374. *Id.*, Art. 71d (1).

375. *Id.*, Art. 71c (2).

376. *UPC Agreement*, *supra* note 16, Art. 63 (1).

destruction,[377] information,[378] and damages.[379] The claimant can also request the publication of the decision at the expense of the defendant.[380]

The enforcement of decisions of the UPC is governed by Article 82 UPCA in connection with Rule 354. Accordingly, any decision of the court shall be enforced under the same conditions as a decision given in the contracting member state where the enforcement takes place. The decisions of the UPC are enforceable in all contracting EU member states, although the enforcement can be made subject to the provision of a security,[381] whether by deposit, bank guarantee, or otherwise.[382] The national law is only applicable to the extent the UPCA and the statute of the court do not prevail.[383]

To the extent the enforcement of acts are subject to the actual cooperation of the defendant (such as the claims for injunctive relief, information, and recall), the enforcement can include recurring penalty payments payable to the court.[384] The amount of the penalty payment "shall be proportionate to the importance of the order to be enforced and shall be without prejudice to the party's right to claim damages or security."[385] The penalty shall be fixed either upon request or of the court's own motion. The defendant's right to be heard shall be observed by either inviting the parties to provide written submissions within

377. *Id.*, Art. 64.

378. *Id.*, Art. 67.

379. *Id.*, Art. 68.

380. *Id.*, Art. 80.

381. *Id.*, Arts. 82(1)–(2).

382. Rule 352(1), UPCA RoP, *supra* note 26.

383. *UPC Agreement*, *supra* note 16, Art. 82(3).

384. *Id.*, Arts. 63(2) & 82(4); Rule 354(3), UPCA RoP, *supra* note 26.

385. *UPC Agreement*, *supra* note 16, Art. 82(4).

a specified period or to an oral hearing on a fixed date.[386] According to views in the literature, there are no sanctions available beyond those specifically stipulated in the UPCA.[387] Thus, there is no jurisdiction for national law or courts. Particularly, there is no room for additional penalty measures (such as detention of the directors as is possible, for example, under German procedural law).

In relation to enforcement of acts that can be conducted by third parties (such as the claims for removal from the channel of distribution and destruction), the court may order that such acts be carried out at the expense of the defendant.[388] Apart from this, penalty payments against third parties for noncompliance are not foreseen by the UPCA. In this regard, it has been suggested that national laws be applicable pursuant to Article 82(3) UPCA.[389]

As regards the enforcement of damage awards, the order of penalty payments is governed by national laws, i.e., by the law of the contracting EU member state in which the enforcement is to be conducted.[390]

386. Rule 354(4), UPCA RoP, *supra* note 26, in connection with Rule 264.

387. Matthias Leistner, *Vollstreckung von Urteilen des Einheitlichen Patentgerichts in Deutschland*, GRUR, Vol. 118, No. 3, 217–25 (2016).

388. *UPC Agreement*, *supra* note 16, Art. 64(3).

389. Michael Nieder, *Vollstreckung des EPG-Verletzungsurteils und Vernichtung des Klagepatents nach Rechtskraft*, GRUR, Vol. 119, No. 1, 38–42 (2017).

390. *UPC Agreement*, *supra* note 16, Art. 82(3).

B. Mitigation possibilities for the defendant

1. Formal requirements of enforcement

Even if Rule 345 UPCA states that decisions and orders of the court are immediately enforceable, Rule 118(8) provides some necessary actions by the interested party.

In particular, the patentee may proceed with enforcement, in respect of individual judgements, only if:

- it has notified the court that it intends to proceed to enforce a determined part of the judgement—indicating which part; and
- it serves this notice together with a certified translation of the notice and of the operative orders of the judgement to be enforced into the official language of the contracting member state in which the enforcement shall take place.

In the absence of the above, the defendant can appropriately oppose the enforcement.

2. Appeal (or rehearing) and suspensive effect

The defendant might prevent the enforcement of an adverse UPC decision through appeal.

Appeals may be brought within a term of two months for court decisions and fifteen days for orders.[391] Generally speaking, the case management of the appeal proceedings is similar to the first instance proceedings:

- Grounds of appeal to be filed within four months after service of decision or fifteen days after service of the order.[392]

391. Rule 224(1), UPCA RoP, *supra* note 26.

392. *Id.*, Rule 224(2).

- Statement of response to be filed within three months or fifteen days, respectively,[393] which may include a statement of cross-appeal.[394]
- Reply to statement of cross-appeal within two months or fifteen days, respectively.[395]
- Interim procedure.[396]
- Oral hearing.

Decisions or orders of first instance may be upheld, reversed, or partially reversed.[397]

Apart from this, an appeal does not have automatic suspensive effect, so the first instance decision may be enforced even if it has been appealed. However, the court of appeal may grant suspensive effect to the appeal procedure following motivated request of one of the parties.[398] The application shall set out why the appeal should have suspensive effect along with the facts, evidence, and arguments relied on.[399] It is specified that the court of appeal shall decide the application without delay.

In the case of extreme urgency, the applicant may without formality and at any time apply to the standing judge for an order for suspensive effect. However, Rule 223 UPCA also states "[t]here shall be no suspensive effect for an appeal of an order pursuant of Rule 220.2." Moreover, Article 74(2) UPCA provides that an appeal against a decision on actions or

393. *Id.*, Rule 235.

394. *Id.*, Rule 237.

395. *Id.*, Rule 238.

396. *Id.*, Rule 239. Interim procedures are similar to first instance proceedings, *see supra* Section IV.B (Available remedies in (main) infringement actions).

397. *Id.*, Rule 242.

398. *UPC Agreement*, *supra* note 16, Art. 74(1).

399. Rule 223, UPCA RoP, *supra* note 26.

counterclaims for revocation and on actions based on Article 32(1)(i)—actions against EPO decisions—shall always have a suspensive effect.

In very exceptional cases, the UPC division can determine during a request of rehearing after a final decision that the decision does not have suspensive effect,[400] but the court of appeal may decide otherwise.[401]

3. Patent revocation or amendment

Where an enforceable decision or order has been made pursuant to a finding of infringement of a patent and, following the conclusion of the action, the patent is amended or revoked, the court may order, upon the request of the party against whom the decision or order would be enforceable, that the decision or order ceases to be enforceable.[402]

4. National enforcement remedies

According to Article 82(3) UPCA, which clarifies that enforcement procedures shall be governed by the law of the contracting member state where the enforcement takes place, national enforcement remedies may be enacted.[403]

5. Security

Another option, which does not prevent the enforcement of the decision but should avoid possible negative consequences

400. *UPC Agreement*, *supra* note 16, Art. 81.

401. Rule 252, UPCA ROP, *supra* note 26.

402. *Id.*, Rule 354(2).

403. For instance, *Vollstreckungsgegenklage* (action to enforcement counterclaim) or *Titelgegenklage* (title counterclaim) pursuant to ZIVILPROZESSORDNUNG [ZPO] [GERMAN CIVIL PROCEDURE CODE] § 767 in Germany; *Opposizione all'esecuzione* pursuant to CODICE DI PROCEDURA CIVILE [C.C.] [ITALIAN CIVIL PROCEDURE CODE], Art. 615 in Italy.

of the enforcement, is requesting a security. The court may make any order or measure subject to a security to be posted by the successful party to the unsuccessful one.[404] If the security is not already specified in the decision, the interested party can file an application to request the granting of a separate order of security.[405] In the absence of the security (when ordered), the enforcement cannot start.

6. Decision by default

When a decision by default is given, the lodging of a request to set aside this decision may induce the court to grant a stay of the enforcement until it has given its decision on the request.[406]

7. Settlement

The parties may, at any time in the course of the proceeding, conclude their case by way of settlement, which shall be confirmed by a decision of the court.[407] This is also possible after a decision, until *res judicata* applies. A settlement prevents the enforcement of the decision.

8. Modification of the infringing product

If the defendant has modified the infringing product and seeks clarification on the scope of a decision with regard to the modification, it may start an action for negative declaratory judgement before the panel that issued the first judgement. In

404. *UPC Agreement*, *supra* note 16, Art. 82(2), and Rule 352, UPCA ROP, *supra* note 26.

405. TILMANN & PLASSMANN, *supra* note 63, at 1771.

406. Rule 356, UPCA ROP, *supra* note 26.

407. *UPC Agreement*, *supra* note 16, Art. 79.

cases of particular urgency, the court may stay the enforcement on a preliminary basis.[408]

9. Protective letter

Even if a protective letter provided by Rule 207 UPCA is not a means to prevent the enforcement of a decision, we refer to it as an option, in case of urgency, that could be effective in avoiding court-issued provisional measures without first hearing the defendant.

C. Remedies for wrongful enforcement

Even though the UPCA tries to avoid the occurrence of the so-called "injunction gap" (i.e., a time gap between the issuance of the injunction and the decision on the validity), it can still occur.[409] Accordingly, it will be possible for a UPC judgement to be preliminarily enforced, only to have the patent subsequently revoked.

The question is how such wrongful enforcement can be rectified. Rule 354(2) UPCA only stipulates that the ongoing enforcement be stopped. The provision of security pursuant to Article 82(2) UPCA only concerns nonfinal decisions,[410] so it does not help the defendant in case of the unjustified enforcement of final infringement decisions. A rehearing is only possible in cases of criminal offenses or fundamental procedural errors.[411] Articles 60(9) and 62(5) and Rule 213(2) only concern provisional measures.

---

408. TILMANN & PLASSMANN, *supra* note 63, at 1780.

409. *See supra* Section III.D (Bifurcated v. nonbifurcated proceedings).

410. Based on the wording of Art. 82(2) UPCA, this provision is not limited to nonfinal decisions. However, there is no reason why this provision should be extended to the enforcement of final decisions.

411. *UPC Agreement*, *supra* note 16, Art. 81.

Other statutory measures are not available. It has been suggested that Articles 60(9) and 62(5) should be applied *mutatis mutandis* (i.e., with the necessary changes being made).[412] It remains to be seen how courts will deal with this issue once it arises. However, these cases will likely be rare, given that it can be expected that courts will decide on infringement and validity in the same proceedings.

412. Klaus Grabinski, *Der Entwurf der Verfahrensordnung für das Einheitliche Patentgericht im Überblick*, GRUR Int, Vol. 62, No. 4, 310–21 (2013).

THE SEDONA CONFERENCE COMMENTARY ON MONETARY REMEDIES IN TRADE SECRET LITIGATION

A Project of The Sedona Conference Working Group (WG12) on Trade Secrets

Author:

The Sedona Conference

Editors-in-Chief:

David Almeling
Victoria Cundiff
James Pooley

Managing Editors:

Jim W. Ko
Casey Mangan

Senior Editors:

David Bohrer
Erik W. Weibust

Contributing Editors:

John Bone
Amy Candido
Christopher Gerardi
Carol Ludington
Matthew Lynde
Alex Reese
Abraham Y. Skoff

WG12 Judicial Advisors:

Hon. Laurel Beeler
Hon. Juliana Earp
Hon. James L. Gale (ret.)

Staff Editor:

David Lumia

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference's Working Group 12. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any organizations to which they may belong, nor do they necessarily represent official positions of The Sedona Conference.

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, click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> The Sedona Conference, *Commentary on Monetary Remedies in Trade Secret Litigation*, 24 SEDONA CONF. J. 349 (2023).

PREFACE

Welcome to the July 2023 Final, Post-Public-Comment Version of *The Sedona Conference Commentary on Monetary Remedies in Trade Secret Litigation*, a project of The Sedona Conference Working Group 12 on Trade Secret Law (WG12). 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 WG12, formed in February 2018, is "to develop consensus and nonpartisan principles for managing trade secret litigation and well-vetted guidelines for consideration in protecting trade secrets, recognizing that every organization has and uses trade secrets, that trade secret disputes frequently intersect with other important public policies such as employee mobility and international trade, and that trade secret disputes are litigated in both state and federal courts." The Working Group consists of members representing all stakeholders in trade secret law and litigation.

The WG12 *Commentary* drafting team was launched in November 2018. Earlier drafts of this publication were a focus of dialogue at the WG12 Annual Meeting in Reston, Virginia, in September 2022, the Sedona Conference on Trade Secrets in Denver, Colorado, in May 2022, the WG12 Annual Meeting in Phoenix, Arizona in December 2021, the WG12 Annual Meeting, Online, in November 2020, the WG12 Annual Meeting in Charlotte, North Carolina, in November 2019, and the WG12 Inaugural Meeting in Los Angeles, California, in November 2018. The editors have reviewed the comments received through the Working Group Series review and comment process.

This *Commentary* represents the collective efforts of many individual contributors. On behalf of The Sedona Conference, I thank in particular David Almeling and Victoria Cundiff, the Vice-Chair and Chair of WG12, and James Pooley, the now Chair Emeritus of WG12, who serve as the Editors-in-Chief of this *Commentary*, and David Bohrer and Erik W. Weibust, who serve as the Senior Editors of this *Commentary*. I also thank everyone else involved for their time and attention during this extensive drafting and editing process, including our Contributing Editors John Bone, Amy Candido, Christopher Gerardi, Carol Ludington, Matthew Lynde, Alex Reese, and Abraham Y. Skoff.

The drafting process for this *Commentary* has also been supported by the Working Group 12 Steering Committee and Judicial Advisors. The statements in this *Commentary* are solely those of the nonjudicial members of the Working Group; they do not represent any judicial endorsement of any recommended practices.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG12 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, data security and privacy liability, patent remedies and damages, and patent litigation best practices. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be.

Craig W. Weinlein
Executive Director
The Sedona Conference
July 2023

TABLE OF CONTENTS

FOREWORD

The available remedies for trade secret misappropriation drive and define litigation on these claims. Recognizing this, The Sedona Conference created drafting teams of its members to identify, organize, and present consensus, nonpartisan principles on available remedies for trade secret misappropriation, which include both nonmonetary and monetary remedies. The previously published *Commentary on Equitable Remedies in Trade Secret Litigation* provides principles for nonmonetary remedies. This *Commentary* provides them for monetary remedies.

The rules for what money a successful trade secret claimant can recover are easy to state but often difficult to apply. This *Commentary* seeks to be a resource to assist parties and decision-makers in addressing monetary remedies and suggests effective methods for determining whether, and in what amount, to award monetary relief for trade secret misappropriation.

To achieve these aims, this *Commentary* focuses on the statutory and decisional law that provides for the three core types of damages in trade secret cases: actual loss, unjust enrichment, and, in many cases, royalties. This *Commentary* also analyzes the difficult issues that must be grappled with regarding such damages, including apportionment, causation, reasonable certainty, the applicability and inapplicability of patent damages law precedent in trade secret cases, and many more.

David Almeling
Victoria Cundiff
James Pooley
Editors-in-Chief and Working Group 12
Steering Committee Vice-Chair, Chair, and Chair Emeritus

David Almeling
David Bohrer
Erik W. Weibust
Senior Editors

MONETARY REMEDIES IN TRADE SECRET LITIGATION PRINCIPLES AT A GLANCE

PRINCIPLE NO. 1 – Monetary remedies should fairly compensate the trade secret owner for damages sustained as a result of misappropriation.

PRINCIPLE NO. 2 – The existence of damages and the measurement of a monetary damages award for misappropriation must not be speculative, but the amount of damages need not be proved with mathematical certainty.

PRINCIPLE NO. 3 – Multiple theories of measuring damages for misappropriation may be applied so long as there is no double counting.

MONETARY REMEDIES IN TRADE SECRET LITIGATION GUIDELINES AT A GLANCE

GUIDELINE NO. 1 – The duration of the trade secret damages period should align with the elimination of defendant's unfair commercial advantage.

GUIDELINE NO. 2 – A trade secret plaintiff bears the burden to prove that defendant's misappropriation was the proximate cause of its damages.

GUIDELINE NO. 3 – In cases where multiple trade secrets are asserted, the trade secret claimant should provide evidence of apportionment of damages or evidence why an apportionment is not appropriate.

GUIDELINE NO. 4 – Claims for trade secret misappropriation and for misuse of confidential information in breach of contractual obligations are not necessarily interchangeable. Liability and remedies under each theory should be analyzed separately.

GUIDELINE NO. 5 – From the outset of a case, the parties should consider all available equitable and monetary remedies, since the parties' positions on equitable remedies will affect their positions on monetary remedies and vice versa.

GUIDELINE NO. 6 – Patent damages law and theory may or may not be applicable in a particular case, and care should be taken before importing patent damages law and theory.

I. INTRODUCTION

There is more variability in the principles and guidance for awarding trade secret damages—and thus more opportunity for ambiguity—than for other areas of intellectual property.

The issue is not a lack of textual definition in trade secret damages law. State legislatures have widely adopted the Uniform Trade Secrets Act's (UTSA) formulation that "damages" may be awarded for "actual loss" or "unjust enrichment" that is "caused by" misappropriation, and that in lieu of other measures a court may "impose[ ] liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret." The Defend Trade Secrets Act's (DTSA) damages provisions borrow the same language.[1] While virtually every state recognizes those three methods—actual loss, unjust enrichment, and royalties—potential confusion arises because statutory phrases and terms are too often cited without adequate discussion of the aims and intended application of the remedies on which the statutory language is based.

Moreover, existing precedent is derived from cases in which courts apply different rules from different states, resulting in a body of law that is far from uniform.[2] The extensive efforts to

1. 18 U.S.C. § 1836(b)(3)(B)(i)-(ii); Uniform Trade Secrets Act (UTSA), § 3(a). As discussed below, New York, unlike other states, has not adopted a version of the UTSA and instead applies New York common law of trade secrets and the Restatement (First) of Torts § 757. New York's view of unjust enrichment is different from the Defend Trade Secrets Act (DTSA) and the UTSA.

2. *See* Telex Corp. v. Int'l Bus. Mach. Corp., 510 F.2d 894, 930 (10th Cir. 1975) ("[U]nfortunately the general law as to the proper measure of damages in a trade secrets case is far from uniform."); Am. Sales Corp. v. Adventure Travel, Inc., 862 F. Supp. 1476, 1479 (E.D. Va. 1994) ("Computing damages in a trade secrets case is not cut and dry."); Litton Sys., Inc. v. Ssangyong Cement Indus. Co., No. C-89-3832 VRW, 1993 WL 317266, at *2 (N.D. Cal. Aug. 19, 1993) (observing that the principles governing trade secret damages "allow

codify and harmonize the common law of trade secrets have not achieved the desired uniformity.[3]

Against this backdrop of uncertainty and less developed guidelines, courts have embraced the flexibility principle advanced by the Fifth Circuit in *University Computing v. Lykes-Youngstown Corp.*, a 1974 pre-UTSA decision applying Georgia common law of trade secrets and the Restatement (First) of Torts, section 757. In the underlying case, the jury awarded damages for trade secret misappropriation despite the absence of any demonstrable losses to the plaintiff or any success in commercializing the misappropriated trade secrets by the defendants. The Fifth Circuit nonetheless affirmed a jury verdict awarding money damages, approving the trial court's instruction to the jury that it should consider what would constitute a reasonable royalty for unrestricted use of the trade secrets. The Fifth Circuit stated that "every [trade secret] case requires a *flexible and imaginative approach* to the problem of damages" and that "each case is controlled by its own peculiar facts and circumstances."[4]

---

broad latitude in fashioning appropriate remedies"); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 45, Reporters' Note (AM. LAW INST. 1995) ("The cases reflect considerable flexibility in the calculation of appropriate monetary relief in trade secret actions."); MODEL JURY INSTRUCTIONS 8.06[4], at 400 (AM. BAR ASS'N, 3d ed. 1996) (in trade secret cases, "lost profits, unjust enrichment, gains, or other benefits are not consistently applied concepts from jurisdiction to jurisdiction, and may be subject to differing standards under various state laws").

3. James Pooley, *The Myth of the Trade Secret Troll: Why the Defend Trade Secrets Act Improves the Protection of Commercial Information*, 23 GEO. MASON L. REV. 1045, 1050 (2016). The efforts to codify and harmonize trade secret law encompass the 1939 Restatement (First) of Torts, section 757, the original and amended UTSA in 1979 and 1985, respectively, and the 1995 Restatement (Third) of Unfair Competition, section 45.

4. Univ. Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 538 (5th Cir. 1974) (emphasis added) (quoting Enter. Mfg. Co. v. Shakespeare Co., 141 F.2d 916, 920 (6th Cir. 1944)).

Flexibility and uniformity can be compatible. The need to stay flexible in measuring trade secret damages will always have a place in the pantheon of governing principles. But in its implementation, flexibility should not be divorced from commercial reality, nor should it dissuade courts and lawyers from seeking to develop and apply a more consistent set of damages principles and guidelines.

In the following sections, this *Commentary* identifies consensus principles and suggests effective methods for determining whether, and in what amount, to award monetary relief for trade secret misappropriation. This *Commentary* expands on and complements the precedent developed over recent decades and describes the key components of the statutory framework for awarding monetary remedies for trade secret misappropriation. The aim is to review the current state of the law, flag potential issues, and suggest defensible methods for measuring damages.

II. AN OVERVIEW OF MONETARY REMEDIES IN TRADE SECRET DISPUTES

A successful claimant in a trade secrets case may recover both the actual loss caused by the misappropriation and the unjust enrichment caused by the misappropriation not computed in the actual loss.[5] An actual loss award is measured by the amount of the loss sustained by the plaintiff due to the misappropriation. An unjust enrichment award is measured by the amount of the benefit conferred on the defendant due to the misappropriation.

Damages caused by misappropriation may also be measured by a reasonable royalty for the defendant's unauthorized disclosure or use of a trade secret.[6] While most states explicitly provide reasonable royalty damages as a separate form of recovery, a handful do not. Further, California and a few other states allow recovery of a reasonable royalty only if damages are not provable by the other methods or if the value of provable damages would be less than the royalty.[7]

These three remedies—actual loss, unjust enrichment, and royalties—are the main damages theories in trade secret law, and each is discussed in detail below.

In addition, exemplary (i.e., punitive) damages are often potentially recoverable,[8] as are attorneys' fees. These are not addressed here but are scheduled to be addressed in a future Commentary by this Working Group.

This overview focuses on the types of damages that apply in most trade secret cases across the three main sources of trade secret law: the Defend Trade Secrets Act (DTSA), the Uniform

5. UTSA § 3(a); DTSA, 18 U.S.C. § 1836(b)(3)(B)(i).

6. UTSA § 3(a); DTSA, 18 U.S.C. § 1836(b)(3)(B)(ii).

7. See the chart and related discussion of state-specific differences in statutory reasonable royalty damages, in the next section.

8. UTSA §§ 3(b) and 4; DTSA, 18 U.S.C §§ 1836(b)(3)(C) and (D).

Trade Secrets Act (UTSA), and common law (which applies primarily to New York, the only state not to adopt the UTSA). To be sure, there are differences among these sources and even more differences in how courts interpret them. Some of those differences are noted in the discussion that follows, but practitioners are encouraged to consult the applicable law in the applicable jurisdiction. For ease of use, this framework is also set forth in the chart form below.

Potential Remedy	DTSA	UTSA	New York
Actual losses	**Yes**	**Yes**	**Yes**
Unjust enrichment	**Yes,** *if no double counting*	**Yes,** *if no double counting*	**No,** *at least as to defendant's avoided development costs and any other gain by defendant that is not used as a proxy for plaintiff's actual losses*

Potential Remedy	DTSA	UTSA	New York
Reasonable royalty	**Yes**	**Yes,** *but only available in certain states if neither actual loss nor unjust enrichment is provable, or if value of such would be less than royalty*	**Yes**
Exemplary damages	**Yes,** *if willful and malicious*	**Yes,** *if willful and malicious*	**Yes,** *if egregious and/or willful and malicious*
Attorneys' Fees	**Yes,** *in certain circumstances*	**Yes,** *in certain circumstances*	**No,** *only if an independent statutory or contractual basis exists*

This *Commentary* uses the term "monetary remedies" to refer to both money damages and restitutionary remedies.

A. Brief Historical Background of Monetary Relief in Trade Secret Cases

Trade secret law remains a relatively recent creation. "Unlike other forms of intellectual property that can trace their origins back several hundreds of years, trade secret law is a creation of state court opinions from the middle of the 19th century."[9] Formal efforts to harmonize trade secret law did not begin until 1939 with the codification of the Restatement (First) of Torts, which established liability for misappropriation of trade secrets.[10] The Restatement's only reference to damages for trade secret misappropriation, however, is found in comment b, which has more to do with the type of trade secret being protected and contrasting between the availability of injunctive relief and damages than any specific measures of damages in the event of proven misappropriation.[11]

Recognizing "the commercial importance of state trade secret law to interstate business," which through the 1960s "ha[d] not developed satisfactorily" either in "less populous and more

---

9. Brian T. Yeh, Cong. Research Serv., R43714, Protection of Trade Secrets: Overview of Current Law and Legislation, at 5 (2016); *see also* Trade Secret, Legal Information Institute, https://www.law.cornell.edu/wex/trade_secret (last visited May 17, 2023) ("Prior the the [sic] development of the UTSA, improper use or disclosure of a trade secret was traditionally a common law tort. Sections 757 and 758 of the Restatement of Torts (1939) set forth the basic principles of trade secret law that were widely adopted by U.S. courts.").

10. RESTATEMENT (FIRST) OF TORTS §§ 757–758 (AM. LAW INST. 1939); *see also* Ramon A. Klitzke, *The Uniform Trade Secrets Act*, 64 MARQ. L. REV. 277, 282 (1980) ("The development of the law of trade secrets, as a creature of the common law, was greatly facilitated by the adoption of sections 757 through 759 (regarding trade secrets and trade information) of the first Restatement of Torts in 1939. The Restatement was the first attempt to enunciate the generally accepted principles of trade secrets law. Its principles became primary authority by adoption in virtually every reported case.").

11. RESTATEMENT (FIRST) OF TORTS §§ 757–758, cmt. b (Am. Law Inst. 1939).

agricultural jurisdictions" or "states in which there has been significant litigation," the National Conference of Commissioners of Uniform State Laws set about to create a uniform body of law. In 1968, it "voted to authorize the appointment of a Special Committee on Uniform Trade Secrets Protection Act to investigate the question of drafting an act on the subject" of trade secret law. After fits and starts, the UTSA was approved on August 9, 1979, and recommended for enactment in all 50 states. Since then, 49 states have adopted the UTSA in one form or another, most recently Massachusetts, which adopted the UTSA in 2018.[12] The lone holdout is New York.

Section 3 of the UTSA sets forth the following framework for measuring damages in the event of a proven misappropriation:

> (a) Except to the extent that a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation renders a monetary recovery inequitable, a complainant is entitled to recover damages for misappropriation. Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss. In lieu of damages measured by any other methods, the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret.
>
> (b) If willful and malicious misappropriation exists, the court may award exemplary damages in

12. UTSA With 1985 Amendments, Prefatory Note, at 1–3; MASS. GEN. LAWS ch. 93, § 42, *et seq*.

> an amount not exceeding twice any award made under subsection (a).

In other words, the UTSA provides for recovery of: (1) actual losses, (2) unjust enrichment, (3) reasonable royalties, and (4) exemplary damages.

The availability of a reasonable royalty as a measure of damages was not explicitly added to the UTSA until it was amended in 1985; it was not in the original version.[13]

Section 4 of the UTSA provides for the recovery of attorneys' fees under certain specified circumstances.

---

13. It is unclear why the original 1979 version of the UTSA did not reference reasonable royalties, particularly because reasonable royalties were used as a measure of damages before its enactment, including in the Fifth Circuit's seminal 1974 *University Computing* decision. *See* Univ. Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 536–41 (5th Cir. 1974) (analyzing availability of reasonable royalty as a measure of damages for trade secret misappropriation and upholding jury instruction permitting award of the same); *see also, e.g.*, Carter Prods., Inc. v. Colgate-Palmolive Co., 214 F. Supp. 383, 388 (D. Md. 1963) ("damages for the misappropriation of the trade secrets as well as for the patent infringement may properly be allowed on the basis of a reasonable royalty"). Curiously, the prefatory note to the UTSA's 1985 amendment attempts to explain this omission by pointing out that "[t]he recent decision in *Aronson v. Quick Point Pencil Co*., 99 S. Ct. 1096, 201 USPQ 1 (1979) reaffirmed *Kewanee* and held that federal patent law is not a barrier to a contract in which someone agrees to pay a continuing royalty in exchange for the disclosure of trade secrets concerning a product," and highlighting the uneven development of trade secret law. *See* UTSA With 1985 Amendments, Prefatory Note, at 1. But the *Aronson* decision did not create a new right to reasonable royalties for proven trade secret misappropriation, so this reference is peculiar. Indeed, the *Kewanee* decision that *Aronson* "reaffirmed" was decided in 1974 and did not even address reasonable royalties, but rather involved preemption. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974) (holding that state law forbidding misappropriation of trade secrets was not preempted by federal patent law).

Unfortunately, the UTSA's codification efforts did not yield all the benefits expected to flow from uniform applications of the law. States adopted slightly different versions of the UTSA. Even where the language is the same, some states interpret it differently than others, which has created state-specific nuances that detract from the UTSA's intended uniformity.[14]

In 2016, Congress enacted the Defend Trade Secrets Act.[15] The DTSA, which amended the Economic Espionage Act, established a private civil cause of action in federal court for trade secret misappropriation. The DTSA's damages provisions (which include actual losses, unjust enrichment, reasonable royalties, and exemplary damages)[16] are "drawn directly" from Section 3 of the UTSA, and the availability of attorneys' fees under the DTSA is "modeled on" Section 4 of the UTSA.[17]

In sum, despite some differences in the applicability of monetary remedies under the DTSA, UTSA, and common law, they at least feature largely consistent forms of recoverable damages.

B. Three Categories of Recoverable Damages

<u>Principle No. 1</u> – Monetary remedies should fairly compensate the trade secret owner for damages sustained as a result of misappropriation.

---

14. For example, the West Virginia Uniform Trade Secrets Act does not include a prohibition on double counting unjust enrichment damages and actual losses. *See* W. VA. CODE § 47-22-3 (2015). There is no right to a jury under the California Uniform Trade Secrets Act on the issue of reasonable royalty, CAL. CIV. CODE § 3426.3(c) (1984), while most other states do permit a jury right. And there is a mixed bag among the states with respect to exemplary damages in terms of the permissible amount and who makes the determination (judge vs. jury).

15. 18 U.S.C. § 1836, *et seq*.

16. 18 U.S.C. § 1836(b)(3)(B).

17. S. REP. NO. 114-220, pt. III., at 8–9 (2016).

When measuring the amount of a monetary remedy, the goal is to provide fair compensation for the losses sustained or the advantages gained as a result of misappropriation. Each of the three methods of measuring damages (actual loss, unjust enrichment, and reasonable royalty damages) provides a lens through which to measure the impact of misappropriation.[18] Actual loss damages is a traditional common law tort remedy[19] measured by the plaintiff's losses due to misappropriation.[20] Unjust enrichment damages aims to prevent the defendant's unjust enrichment and is measured by defendant's gain due to misappropriation.[21] Reasonable royalty damages aim to derive a usage-based payment that would have been set in a hypothetical negotiation between the trade secret owner (as a willing licensor) and the misappropriator (as a willing licensee) for the misappropriator's use of a trade secret.[22]

---

18. As discussed below, the failure to provide sufficient evidence tying any of these measurements to misappropriation may cause a court to exclude them as unduly speculative and unreliable.

19. *See* RESTATEMENT (SECOND) OF TORTS §§ 901 cmt. a, 902, 903, 906 (AM. LAW INST. 1979) ("This first purpose of tort law leads to compensatory damages").

20. UTSA § 3(a); DTSA § 1836(b)(3)(B).

21. UTSA § 3(a); DTSA § 1836(b)(3)(B). A potential source of confusion is that restitution law provides both a free-standing substantive basis for establishing liability (e.g., as a stand-alone claim asserting unjust enrichment) and as is the case with trade secret misappropriation, an alternate available remedy. DAN B. DOBBS & CAPRICE L. ROBERTS, LAW OF REMEDIES: DAMAGES, EQUITY, RESTITUTION § 4.1, at 370 (3d ed. 2018) ("Restitution remedies may flow from a freestanding cause of action based on unjust enrichment or may piggyback on other causes of action such as contracts, torts, fiduciary duties, and intellectual property.").

22. In some instances, the determination of a reasonable royalty may be presented as an approximation of plaintiff's lost revenue or other actual losses, *see* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 45 cmt. b (AM. LAW INST. 1975), or as an approximation of defendant's avoided costs of

That there are several types of potentially available methods for measuring damages reflects the need for flexibility in calculating misappropriation damages.[23] For example, depending upon the circumstances in a specific case, it may be difficult to establish the existence or amount of the plaintiff's actual losses or the defendant's unjust enrichment. In most jurisdictions, these different approaches are not exclusive of one another, and a plaintiff may elect a hybrid measurement of its damages based on one or more approach.[24]

1. Actual loss

The DTSA, every state's version of the UTSA, and New York common law all explicitly provide for the recovery of damages for actual loss caused by trade secret misappropriation. Actual loss is a measure of harm caused to the plaintiff, as opposed to gains or unjust enrichment benefiting the defendant (which is addressed in the next section). The goal of awarding damages

---

developing a competing product or other unjust enrichment, *see id*. cmt. g, and BladeRoom Grp. Ltd. v. Facebook, Inc., No. 5:15-CV-01370-EJD, 2018 WL 1611835 (N.D. Cal. Apr. 3, 2018) (defendant's expert properly used reasonable royalty method to measure defendant's unjust enrichment from unauthorized use of the trade secret (applying California's version of UTSA), *rev'd on other grounds*, 11 F.4th 1010 (9th Cir. 2021)).

23. Univ. Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 536–39 (5th Cir. 1974); *see also* Bohnsack v. Varco, L.P., 668 F.3d 262, 280 (5th Cir. 2012) (noting that the variety of approaches to trade secret damages "demonstrates the 'flexible' approach used to calculate damages for claims of misappropriation of trade secrets" (citation omitted)).

24. *See, e.g.*, Agilent Techs., Inc. v. Kirkland, No. 3512-VCS, 2010 WL 610725, at *28–31 (Del. Ch. Feb. 18, 2010) (applying the Delaware enactment of the UTSA, the court's award combined consistent lost profit damages and unjust enrichment damages).

for actual loss is to compensate the plaintiff for any harm caused by the defendant.[25]

Although "actual losses" are often thought of as "lost sales" or "lost profits," the concept is broader than that. Actual loss may be measured in various ways, including (a) lost profits (both past and demonstrable/nonspeculative future lost profits) from lost sales or price erosion; (b) increased costs incurred as a result of the misappropriation (sometimes set forth as a separate measure of actual loss or sometimes used as a measure of lost profits); (c) lost royalties (whether in the form of a fully paid up lump-sum payment for access to the trade secrets or a running royalty for the misappropriator's use); and (d) diminution or destruction of value (either of the trade secret claimant's business or of the trade secret itself).

a. Lost profits

Lost profits are among the most common measures of actual loss.[26] Lost profits often result from diverted sales or price erosion.[27]

---

25. *See supra* Section II(B)(1) for a discussion of actual losses as a damages remedy.

26. *See* West Plains, L.L.C. v. Retzlaff Grain Co., No. 8:13-CV-47, 2016 WL 165698, at *2 (D. Neb. 2016) ("The Court recognizes that lost profits and unjust enrichment are the most common methods to measure damages in misappropriation cases.") (citing, *inter alia*, DeVries v. Starr, 393 F.2d 9, 19 (10th Cir. 1968) ("Loss of profits, where reasonably ascertainable, have been the usual measure of compensatory damages in cases like these.")); *see also Agilent Techs.*, 2010 WL 610725, at *27 ("The loss suffered by the plaintiff, such as lost profits, is the usual indicator of damage").

27. The term "lost profits" is at times used in this *Commentary* to refer to lost profits from lost sales or price erosion. However, "lost profits" may also be used to refer to other forms of actual loss such as increased costs incurred as a result of the misappropriation. *See*, *e.g.*, Cacique, Inc. v. Stella Foods, Inc., No. B139433, 2002 WL 705675, at *6 (Cal. Ct. App. Apr. 24, 2002) (noting that

Lost profits are not always an appropriate measure of trade secret damages; they must be proved, case by case. One underlying theory of lost profits damages is that "but for" the defendant's misappropriation of trade secrets, the plaintiff would have achieved a higher level of profits by making all, or some, of the sales diverted by the defendant. Such a theory may not be viable if the plaintiff cannot establish a causal link between the lost profits and the misappropriation. Moreover, a plaintiff is unlikely to establish lost sales under this theory if, for example, the trade secret owner would not have been able to procure, manufacture, market, sell, and finance the products or services necessary to generate a profit on defendant's sales—because, say, the trade secret owner lacked the marketing or manufacturing capacity to do so. Any lost profits calculation also must be based on an adequately supported damages period and account for other factors that could have caused some portion of the harm independent of the misappropriation.

Lost sales. In the case of lost sales, lost profits are typically calculated by determining lost revenue and then deducting the incremental or avoided costs that would have been incurred in producing the lost revenue. Lost revenue is generally the difference between the plaintiff's actual revenue during the loss period and the but-for revenue. Lost revenue derives from sales shown to have been diverted by the misappropriation; if the misappropriation prevented the plaintiff from making sales, the profits that would have flowed from those sales are diverted (i.e., lost). After determining the amount of lost revenue, the

---

"the owner of trade secrets who has been victimized by misappropriation of its trade secrets may suffer lost profits because the owner did not make sales that were diverted to the wrongdoer, or the owner incurred increased expenses in connection with the sales that it did make, or the owner cut its prices to compete with the wrongdoer") (citing Lam, Inc. v. Johns-Manville Corp., 718 F. 2d 1056, 1065 (Fed. Cir. 1983) ("Lost profits may be in the form of diverted sales, eroded prices, or increased expenses.")).

costs that the plaintiff would have incurred to generate that revenue (also called incremental or avoided costs) must be calculated. These incremental or avoided costs are then subtracted from the lost revenue to calculate lost profits.

Lost revenue. Determining lost revenue can be challenging. One approach is to focus on the defendant's actual sales and determine what portion of those sales was diverted as a result of the misappropriation. Another approach is to establish the trade secret owner's but-for revenues (i.e., those revenues that the trade secret owner would have made but for the trade secret misappropriation). A difference between the but-for and actual revenues may be lost revenues attributed to the trade secret misappropriation (assuming that a causal link is properly established). But-for revenue may be determined in various ways, such as by looking at the parties' actual sales before, during, and after the damages period (information typically available from the parties' financial and business records), market information and analysis, business plans, capacity considerations, and other factors that could have affected the plaintiff's level of revenues. Market structure may also impact these calculations. For example, in multiplayer markets where competing products do not rely on the trade secrets at issue, a plaintiff must, as part of its causation case, provide some reasonable evidence that customers would have bought from it rather than its competitors to establish a lost profits theory.[28] In determining but-for sales in a

28. *See, e.g.*, Allied Erecting & Dismantling Co. v. Genesis Equip. & Mfg., Inc., 511 F. App'x 398, 404 (6th Cir. 2013) (finding no error in jury instruction requiring plaintiff to show that customers would have purchased its products but for the misappropriation); Suburban Graphics Supply Corp. v. Nagle, 5 A.D.3d 663, 666 (N.Y. App. Div. 2004) (lost profits limited to those "resulting from the defendant's actual diverting" of customers) (quoting Allan Dampf, P.C. v. Bloom, 127 A.D.2d 719, 720 (N.Y. App. Div. 1987)). This evidence can take the form of a market share analysis. *See* Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc., 35 F.3d 1226, 1245 (8th Cir. 1994) ("The court relied on

multiplayer market, it may be appropriate to consider the plaintiff's market share of the properly defined relevant market.

Lost profits are then calculated by subtracting incremental costs from the lost revenue. Incremental or avoided costs are the costs associated with producing and selling the claimed lost sales volume. An obvious example of an incremental cost is material used to produce a product. Other production costs, as well as certain selling and marketing expenses, may also be incremental. Determining which costs are incremental, and their amount, may be informed by such factors as the parties' actual cost detail (including detail of cost of goods sold and operating expenses); an understanding of which costs are fixed, variable, or semivariable; and various analytical approaches.

Price erosion. Price erosion damages may be available when "a defendant's misappropriation enabled it to enter the market and compete directly with the plaintiff," and the plaintiff lowered its prices (or was unable to pass along price increases) as a result.[29] Price erosion damages may be available even if there are multiple players in the same product market, so long as the plaintiff's adverse pricing impacts are the result of

---

Holden's actual sales figures, the known productive capacity of Pioneer's parent lines, Pioneer's profitability history and a reasonable estimate of Pioneer's lost share of the 'look-alike' market.").

29. Stanacard, LLC v. Rubard LLC, No. 12-Civ.-5176 (CM), 2016 WL 6820741, at *2 (S.D.N.Y. Nov. 10, 2016) (refusing to exclude expert testimony on price erosion damages). Note that merely showing the defendant misappropriated and competed may not be sufficient; some evidence that the unlawful competition actually motivated the plaintiff to reduce its prices appears to be necessary. *See In re* Jonatzke, 478 B.R. 846, 866 (Bankr. E.D. Mich. 2012) (finding insufficient evidence of price erosion where expert merely "assume[d] that any erosion . . . must have been because of" the misappropriation).

misappropriation.[30] Price erosion damages may include both past losses and projected future losses caused by the misappropriation.[31]

The underlying theory of lost profits from price erosion is that "but for" the defendant's misappropriation of trade secrets, the plaintiff would have sold its product(s) at higher prices than it actually did (either because it lowered its prices or could not increase its prices because of the defendant's misappropriation). Lost profits from price erosion are typically calculated by subtracting the plaintiff's actual revenue from its but-for revenue without price erosion for the applicable damages period. Again, this math is simple, but determining and supporting the inputs typically may require actual data from both parties (and possibly others), market information, evidence to demonstrate a causal link between the misappropriation and pricing impacts, and other information and analysis. Actual sales volume, prices, and revenue are typically available from the parties' financial and business records. The analysis of price erosion may be facilitated by sales detail such as customer detail, detail of sales by product, detail of sales by month (or other frequencies), price exception

30. Roton Barrier, Inc. v. Stanley Works, 79 F.3d 1112, 1120 (Fed. Cir. 1996) ("Roton reduced its prices in response to Stanley's entry in the market. Though there were others in the market, Zero and Pemko, with lower prices, Roton perceived their products to be inferior and saw no need to lower its prices in response to their entry."); *but see* PQ Labs, Inc. v. Yang Qi, No. 12-0450 CW, 2014 WL 4954161, at *5 (N.D. Cal. Sept. 30, 2014) (holding that evidence admitted during bench trial did not support price erosion damages because, among other things, it "ignore[d] numerous other competitors in the market").

31. *Roton Barrier*, 79 F.3d at 1120 (affirming both past and future price erosion damages). As to future price erosion damages, the court found that testimony showing that the plaintiff would need a "period of time" to "reestablish its prices and margins" was sufficient to sustain the damages awarded by the trial court. *Id.*

reports or other documents reflecting price adjustments made and reasons for them, and market information. Supporting a price erosion claim may also be assisted by information from other competitors, customers, market information, and other analysis. For example, one important analytical issue with price erosion claims is the need to assess the sensitivity of customer purchases to higher prices (i.e., whether and to what extent customers would have purchased the same volume of goods at the claimed higher prices). Because price erosion claims assert that a claimant's prices would have been higher but for the erosion, it is important to consider whether there are sales that would not have been made at the higher prices and remove them from the lost sales/profits analysis. That can be accomplished by measuring the price elasticity of demand.[32] Price erosion calculations typically also consider other potential supply or demand drivers that could have pushed prices down, such as the entrance of new competitors into the relevant market, the introduction of new suitable nonaccused alternative products, or changing customer preferences, among other factors.[33] The information and analysis appropriate to address price erosion will differ based on the facts and circumstances of each situation.

Where a plaintiff obtains an injunction against the misappropriator's sales, the amount and duration of price erosion may be lessened. But an injunction may not immediately end a price erosion damage claim. Even after an injunction, a plaintiff sometimes may not be able to return its prices to levels that would

32. Price elasticity of demand is a measure of the change in the quantity demanded or purchased of a product in relation to its price change. Expressed mathematically, it may be expressed as Price Elasticity of Demand = Percent Change in Quantity Demanded divided by Percent Change in Price.

33. *See Roton Barrier*, 79 F.3d at 1120; *Stanacard*, 2016 WL 6820741, at *2 (refusing to exclude expert testimony on price erosion and holding that arguments about "market factors" went to the weight of the expert's testimony).

have existed but for the misappropriation. As a result, price erosion damages may continue during a postinjunction period.

b. Increased costs or expenses

Another measure of actual loss damages is the increased costs or expenses that the plaintiff incurred as a result of the defendant's misappropriation.[34] As noted above, sometimes these costs or expenses are simply included in the calculation of lost profits. When that occurs, care should be taken to avoid double counting.

To be recoverable, a plaintiff must first prove that the increased costs or expenses were proximately caused by the misappropriation.[35] Be aware, however, that the cost of

34. *See, e.g.*, Food Services of America, Inc. v. Carrington, No. CV-12-00175-PHX-GMS, 2013 WL 4507593, at *14 (D. Ariz. Aug. 23, 2013) ("The Arizona Supreme Court has stated that when the wrongful act of a defendant 'makes it necessary to incur expense to protect [the plaintiff's] interest, such costs and expenses . . . should be treated as the legal consequences of the original wrongful act and may be recovered as damages.'" (citing U.S. Fid. & Guar. Co. v. Frohmiller, 71 Ariz. 377, 380 (Ariz. 1951)). Other state courts determining damages under statutes modeled after the UTSA have found "out-of-pocket expenses" sustained as a result of misappropriation to be an element of damages. *See, e.g.*, Dozor Agency, Inc. v. Rosenberg, 218 A.2d 583, 585–86 (Pa. 1966); Telex Corp., v. Int'l Bus. Mach. Corp., 510 F.2d 894, 931 (10th Cir. 1975) (noting that expenses incurred in strengthening security measures after misappropriation would be damages in some circumstances)); *see also* Synergetics, Inc. v. Hurst, 477 F.3d 949, 960 (8th Cir. 2007) (affirming award of damages including out-of-pocket expenses).

35. *See* Computer Sciences Corp. v. Computer Assocs. Int'l, Inc., Nos. CV 98-1374-WMB SHX, CV 98-1440-WMB SHX, 1999 WL 675446, at *13 (C.D. Cal. Aug. 12, 1999) ("CSC musters little response to CA's causation argument beyond citing cases in which courts have upheld as damages expenses incurred by a plaintiff in protecting itself against actions taken by those who had misappropriated its trade secrets . . . . These cases merely identify the types of expenses that can be proximately caused by a misappropriation of trade

investigating *whether* there was misappropriation or damage caused by increased costs or expenses is not necessarily recoverable, particularly where there is no evidence that the defendant actually used the trade secrets.[36] Accordingly, sufficient information and analysis needs to be gathered and presented to demonstrate a causal link between the misappropriation and increased costs.

c. Research & development costs

Some courts have used a plaintiff's development costs as a measure of the plaintiff's actual loss resulting from misappropriation. "The cost to create property has long been considered an appropriate factor in computing damages, so long as the 'property . . . is injured or destroyed by the wrongful or negligent act of another.'"[37] But there are exceptions and qualifications. For example, one court "excluded expert testimony purporting to measure damages by R&D costs, noting that such costs do not bear a necessary relation to the market value of the research once developed," and holding that "the 'cost to create or duplicate' method could generate the same value for a worthless trade

secrets; they do nothing to eviscerate the requirement that a defendant's wrongful acts be a 'but for' cause of plaintiff's damages.") (citations omitted).

36. *See*, *e.g.*, News Am. Mktg. In-Store, Inc. v. Marquis, 862 A.2d 837, 846 (Conn. App. Ct. 2004) (distinguishing *Dozor*, 218 A.2d 583, on the grounds that in *News Am.*, no use was established, and the out-of-pocket expenses awarded in *Dozor* "were incurred by the plaintiff while attempting to mitigate and reverse the harm actually caused by the defendant's conduct," whereas in this case, "the 'out-of-pocket expenses' suffered by the plaintiff amount to nothing more than costs incurred in the course of investigating whether the plaintiff had suffered an injury as a result of [the defendant's] misconduct.").

37. W.L. Gore & Assoc., Inc. v. GI Dynamics, Inc., 872 F. Supp. 2d 883, 892 (D. Ariz. 2012) (quoting Universal Pictures Co. v. Harold Lloyd Corp., 162 F.2d 354, 370 (9th Cir. 1947)).

secret and a trade secret worth millions of dollars."[38] And some courts, including the Fifth Circuit in *University Computing v. Lykes-Youngstown Corp.*, have held that research and development costs are recoverable only where the entire value of the trade secret has been destroyed, such as where the trade secret was publicly disclosed.[39] In other cases, "where the trade secrets developed by the research have been demonstrated to have actual value . . . courts have measured damages, at least in part, by development costs."[40]

---

38. *Id.* (citing Applied Hydrogel Tech., Inc. v. Raymedica, Inc., No. 06-CV-2254-DMS-POR, 2008 WL 5500756, at *2 (S.D. Cal. Oct. 7, 2008)).

39. *See, e.g.*, Univ. Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 538 (5th Cir. 1974) ("This measure of damages simply uses the plaintiff's actual costs, and in our view is frequently inadequate in that it fails to take into account the commercial context in which the misappropriation occurred."); Softel, Inc. v. Dragon Med. and Sci. Commc'ns, Inc., 118 F.3d 955, 969 (2d Cir. 1997) (rejecting claim that plaintiff was entitled to R&D costs as a measure of damages, because "[h]ere, Dragon did not publish Softel's secrets, and therefore did not destroy their value to Softel, other than to the extent that Dragon itself used them."); Telecom Tech. Servs., Inc. v. Siemens Rolm Commc'ns, Inc., No. 1:95-CV-00649-WBH, 2000 WL 35568637, at *8 n.16 (N.D. Ga. July 26, 2000) ("The broad measure of damages advocated by Rolm [including R&D costs] is available only where the value of the trade secret is completely destroyed, such as where general disclosure to the public occurs, or where unjust enrichment calculations are speculative, neither of which occurred here.").

40. *W.L. Gore & Assoc.*, 872 F. Supp. 2d at 892 (citing Telex Corp. v. Int'l Bus. Mach. Corp., 510 F.2d 894, 931 (10th Cir. 1975) (affirming a damages award based on research costs when "the trial court first found that IBM had expended $10,000,000 on the development of the Aspen project . . . and that Gruver and others had left IBM half way through the development program")); *see also, e.g.*, Leatt Corp. v. Innovative Safety Tech., LLC, 09-CV-1301-IEG-BGS, 2010 WL 11442713, at *5 (S.D. Cal. Aug. 24, 2010) (finding plaintiff's claimed R&D costs to be "an appropriate substitute of [plaintiff's] actual losses due to the misappropriation").

Companies typically track R&D expenditures and often maintain R&D time records with descriptions of projects, technologies, or other relevant details. These records may be useful in identifying development time and expenditures related to asserted trade secrets, particularly where the asserted trade secrets represent a plaintiff's primary technology. But asserted trade secrets often relate to only a portion of a company's technology, development time, and development efforts. In these situations, a company's R&D records commonly do not identify time or expenditures by specific trade secret, and tracing these expenditures to the specific trade secrets at issue in a particular litigation may prove challenging (making apportionment determinations more challenging as well). Therefore, additional analysis, estimates, or other information may be necessary to quantify and adequately support development costs related to asserted trade secrets.

d. Diminution or destruction of value

Value is often defined as the price that a reasonable buyer or investor would pay for a business or asset and/or the value to the owner of being able to sell or license the asset. The American Society of Appraisers Business Valuation Standards Glossary defines fair market value as:

> The price, expressed in terms of cash equivalents, at which property would change hands between a hypothetical willing and able buyer and a hypothetical willing and able seller, acting at arm's length, in an open and unrestricted market, when neither is under compulsion to buy or sell and

> when both have reasonable knowledge of the relevant facts.[41]

Diminution or destruction of value in trade secret misappropriation damages is often addressed as the diminution or destruction of either (1) the value of a business or (2) the value of a trade secret. (There can also be other value-based actual loss theories, such as the value of a lost business opportunity.)

Business value. In certain circumstances, trade secret plaintiffs may prove damages based on diminution or destruction of a business's value caused by misappropriation. This measure of damages "focuses upon the change in worth of a going concern after total or almost total destruction" caused by misappropriation.[42]

A leading case approving this theory is *Wellogix, Inc. v. Accenture LLP*, which involved the defendant's misappropriation of Wellogix's software. At trial, the plaintiff's damages expert valued its damages at $27.8 million, based partly on an $8.5 million investment in Wellogix by venture capital groups in exchange for a 31 percent equity stake.[43] The plaintiff's software expert testified that "the total value of Wellogix went to zero" after the alleged misappropriation.[44] According to its CEO, Wellogix was the only company offering that type of software from 2000 to 2005.[45] The jury awarded $26.2 million in compensatory

---

41. *International Glossary of Business Valuation Terms*, NAT'L ASS'N OF CERTIFIED VALUATORS AND ANALYSTS (June 08, 2001), https://www.nacva.com/content.asp?contentid=166.

42. C. A. May Marine Supply Co. v. Brunswick Corp., 649 F.2d 1049, 1053 (5th Cir. 1981). Note that the court in *May Marine* was discussing loss of business value as a measure of damages for breach of contract, not trade secret misappropriation.

43. 716 F.3d 867, 879 (5th Cir. 2013).

44. *Id*. at 880.

45. *Id*. at 873.

damages, which the Fifth Circuit upheld on appeal, emphasizing the "'flexible' approach used to calculate damages for claims of misappropriation of trade secrets."[46] Other courts have also acknowledged that loss or destruction of business value may be an appropriate measure of damages in trade secrets cases.[47]

As demonstrated by *Wellogix*, value estimates can be facilitated by the existence of offers to invest or valuations done for nonlitigation purposes. In these circumstances, it is important to establish the nexus between the value estimates and the asserted trade secrets (versus other factors that may have contributed to the valuation) and/or to demonstrate that the misappropriation was the cause of the loss or destruction of value.

Trade secret value. Plaintiffs in trade secrets cases may also pursue damages based on the destruction or diminution of the fair market value of the trade secret itself.[48] For example, in

---

46. *Id*. at 880 (quoting Bohnsack v. Varco, L.P., 668 F.3d 262, 280 (5th Cir. 2012)); *see also* Vianet Grp. PLC v. Tap Acquisition, Inc., No. 3:14-CV-3601-B, 2016 WL 4368302, at *22 (N.D. Tex. Aug. 16, 2016) (citing *Wellogix* and denying summary judgment as to a destruction of business value theory).

47. *See, e.g.*, Keystone Transportation Sols., LLC v. Nw. Hardwoods, Inc., No. 5:18-CV-00039, 2019 WL 1770162, at *5 (W.D. Va. Apr. 22, 2019) (refusing to exclude expert opinion on lost business value); CardioVention, Inc. v. Medtronic, Inc., 483 F. Supp. 2d 830, 845–46 (D. Minn. 2007) (refusing to exclude expert opinion on damages that the court described variously as "loss of business value damages" and "the value of the loss of the secret"); Matter of Mandel, 720 F. App'x 186, 188 (5th Cir. 2018) (approving a "lost asset" damages theory based on the value of "companies comparable" to the plaintiff).

48. *See, e.g.*, Univ. Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 535 (5th Cir. 1974) ("[N]ormally the value of the secret to the plaintiff is an appropriate measure of damages only when the defendant has *in some way* destroyed the value of the secret. The most obvious way this is done is through publication, so that no secret remains. Where the plaintiff retains the use of the secret, as here, and where there has been no effective disclosure of the secret through publication *the total value* of the secret to the plaintiff is an inappropriate measure.") (emphasis added) (citations omitted); *see also*

Quintel Technology v. Huawei Technologies USA, the court permitted a damages expert to offer testimony quantifying trade secret misappropriation damages "in terms of [plaintiff's] actual loss as measured by the investment value of the trade secrets at issue."[49] The expert calculated "what a reasonable investor would have paid for the secrets, using detailed development cost information provided by [plaintiff] and applying a price-to-book ratio based upon market reports."[50] Some courts do not recognize this measure of damages, however, and it can be difficult to quantify.[51]

In the case of a start-up or emerging technology company, the company's valuation is closely tied to the value of its trade

---

Precision Plating & Metal Finishing Inc. v. Martin-Marietta Corp., 435 F.2d 1262, 1263–64 (5th Cir. 1970) (upholding award of fair market value of trade secret where that value was completely destroyed); Joe N. Pratt Ins. v. Doane, No. V-07-07, 2009 WL 3157337, at *10 (S.D. Tex. Sept. 25, 2009) ("When utilizing the 'market value' measure of damages, the trier of fact can measure damages based upon what a reasonably prudent investor would have paid for the trade secret." (citation omitted)).

49. No. 4:15-CV-307, 2018 WL 626355, at *8 (E.D. Tex. Jan. 30, 2018), *order clarified*, 2018 WL 6930270 (E.D. Tex. Feb. 27, 2018).

50. *Id.* at *8.

51. *See, e.g.*, Resdev, LLC v. Lot Builders Ass'n Inc., No. 6:04-CV-01374-GAP-DAB, 2005 WL 1924743, at *4 (M.D. Fla. Aug. 10, 2005) (rejecting the argument that diminution of a trade secret's value constitutes "loss"); GTAT Corp. v. Fero, No. CV-17-55-M-DWM, 2017 WL 2303973, at *6 (D. Mont. May 25, 2017) (noting that "the diminution in the value of trade secrets and confidential information cannot generally be addressed through the payment of damages"); Wellness Coaches USA, LLC v. MGM Resorts Int'l, No. 2:15-CV-01593-JAD-CWH, 2015 WL5146701, at *6 (D. Nev. Sept. 1, 2015) ("[L]oss of a property interest in and diminution in value of trade secrets and confidential information are the types of harms that are not readily addressed through payment of economic damages"); Medtronic MiniMed, Inc. v. Nova Biomedical Corp., No. CV-08-00788-SJO-PJWx, 2009 WL 10670877, at *10 (C.D. Cal. Aug. 18, 2009) (excluding evidence of diminution in value of plaintiff's trade secret).

secret technology, and the company's investment value may be tantamount to or at least closely related to the investment value of the trade secret. In some cases, the investment value may be reflected in the total value of the business minus its tangible assets or its ability to raise venture capital. In cases where the business value is destroyed or almost destroyed by the misappropriation, the "investment value" and "lost business value" may be one and the same.

2. Unjust enrichment

Whereas an actual loss reflects the amount of the plaintiff's loss due to misappropriation, unjust enrichment measures the benefit conferred on the defendant due to the misappropriation. The UTSA and the DTSA both provide unjust enrichment damages as a remedy for trade secret misappropriation. Under the UTSA § 3(a) (1985): "Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing damages for actual loss." Under the DTSA, the complainant may recover "damages for any unjust enrichment caused by the misappropriation of the trade secret that is not addressed in computing damages for actual loss."[52]

Unjust enrichment can take many forms. "Simply put," the Seventh Circuit recently concluded, "there is no single way to measure the benefit conferred on a defendant; the measurement is context dependent. The important considerations are that a judge or jury calculates the benefit to the defendant—not the loss to the plaintiff—and that this calculation is done with reasonable certainty."[53] While the considerations vary, certain categories of

52. 18 U.S.C. § 1836(b)(3)(B)(i)(II).

53. Epic Sys. Corp. v. Tata Consultancy Servs., 980 F.3d 1117, 1130 (7th Cir. 2020).

unjust enrichment remedies arise repeatedly: defendant's profits, avoided development costs, and commercial advantage or head-start benefit. (Potential categories also include defendants' increased profitability or market share caused by the misappropriation, defendants' total value if caused by the misappropriation, and others.)

One category of unjust enrichment is sales by defendant that, absent the misappropriation, would not have been made by defendant.[54] Where a plaintiff can prove that the defendant would not have achieved these sales but for the misappropriation, the defendant has been unjustly enriched.

Unjust enrichment damages can also reflect the development costs the defendant avoided through the misappropriation.[55] Plaintiffs have succeeded in obtaining major awards on this

54. These unjust enrichment damages may include both diverted sales and nondiverted sales. Diverted sales are sales by defendant that would have instead been made by plaintiff but for the misappropriation. To the extent these sales are also included in a plaintiff's lost profits claim, care should be taken to avoid double-counting. Nondiverted sales are sales by defendant that, absent the misappropriation, would not have been made by plaintiff. These also represent unjust enrichment sales.

55. *E.g.*, GlobeRanger Corp. v. Software AG US of America, Inc., 836 F.3d 477, 499 (5th Cir. 2016) (plaintiff awarded $19.7 million in development costs avoided by defendant); SW Energy Prod. Co. v. Berry-Helfand, 491 S.W.3d 699, 710–11 (Tex. 2016) ("development costs the defendant avoided by the misappropriation" recognized as basis for damages). *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 45 cmts. f, d (AM. LAW INST. 1995); Univ. Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 535–36 (5th Cir. 1974). *See also*, *Epic Sys.*, 980 F.3d at 1130 ("avoided research and development costs have been awarded when the defendants gained a significant head start in their operations").

basis.[56] There is, however, conflicting authority on the viability and applicability of this measure of damages.[57]

Focusing solely on the measure of overall profits, there is a circuit split over the appropriate measure of a defendant's profits, and courts may consider various setoffs that the defendant properly establishes. Guidance is mixed on the nature and required strength of the nexus between costs and incremental revenues in unjust enrichment calculations. For example, when courts allow costs to be included because they have a "sufficient nexus" to the incremental revenues, disagreement routinely emerges about what that term means. While some courts adopt the incremental approach, others adopt the full absorption method, by which some allocated portion of overhead expenses may be added to incremental expenses to determine the costs to be subtracted. When the law requires that allocations be made—or at least where doing so is an option—a variety of approaches can be used to determine what costs should be subtracted.

Another category of unjust enrichment damages is the benefit to the defendant of being able to develop a competing business or product faster than would have been possible absent misappropriation. The rationale for this type of recovery is that the

56. *E.g.*, Judgment, ASML US Inc. v. XTAL, No. 16-CV-295051 (Santa Clara Super. Ct., May 3, 2019) (plaintiff awarded $845 million for defendant's saved development costs); *Epic Sys.*, 980 F.3d at 1130 ($140 million in saved development costs where defendants obtained a head start through the misappropriation).

57. *Compare Epic Systems* (upholding a $140 million award based on avoided costs and the associated head start that the defendant achieved through misappropriation) *with Syntel Sterling Best Shores Mauritius Ltd. v. The TriZetto Grp., Inc.*, No. 21-1370, 2023 WL 3636674, at *17 (2d Cir. May 25, 2023) (vacating a $285 million award based on avoided costs as "unavailable under the specific facts of this case" because, in part, the plaintiff "suffered no compensable harm beyond that actual loss").

misappropriation has given the defendant an unfair temporal advantage over its competitors. Specific examples include:

- Plaintiff awarded damages measured by defendant's incremental profits on sales over a period of time representative of the research and development time the misappropriation allowed defendant to bypass.[58]
- Defendant required to disgorge damages based on the increased value of defendant's company due to being two years further along than it otherwise would have been in developing and commercializing its products.[59]
- Plaintiff awarded damages based on defendant's profits on sales that began one year earlier than would have been possible without misappropriation—and without which the defendant could not have launched its product at a key trade show.[60]
- Plaintiff entitled to recover damages measured by defendant's profits during a three-year head start on developing a competitive bid and business model for fixed-wing aircraft market'.[61]

---

58. Sensormatic Elecs. Corp. v. Tag Co. US, 632 F. Supp. 2d 1147, 1187 (S.D. Fla. 2008).

59. Sabre GLBL, Inc. v. Shan, 779 Fed. App'x 843, 851 (3d Cir. 2019).

60. Alifax Holding Spa v. Alcor Sci. Inc., 404 F. Supp. 3d 552, 556 (D.R.I. 2019) (court denied renewed Rule 50 motion for judgment as matter of law and accepted and applied head-start damage theory but granted Rule 59 new trial on damages due to potentially prejudicial errors in the admission of supporting proofs).

61. TKC Aerospace. Inc. v. Phoenix Heliparts, Inc., No. CV-2011-018889, 2015 Ariz. Super. LEXIS 981, at *1 (Ariz. Super. Ct. Jan. 30, 2015) (court

This "head start" approach, often referred to as "lead time" damages, is widely followed.[62] Similar to the application of damages measurement rules, the determination of the head-start period is highly dependent on the facts of each particular case.[63]

---

accepted head-start damages theory but deemed the underlying evidence of defendant's profits not sufficiently reliable to support such an award).

62. *See, e.g.*, Nite Glow Indus. Inc. v. Cent. Garden & Pet Co., Nos. 2020-1897, 2020-1983, 2021 WL 2945556, at *6–8 (Fed. Cir. July 14, 2021) (reversing award of $11 million for misappropriation of idea claim brought under New Jersey common law; looking to trade secret misappropriation law for guidance, the Federal Circuit found that plaintiff had failed to provide evidence attributing the award to head-start damages); Tex. Advanced Optoelectronic Sols., Inc. v. Renesas Elecs. Am., Inc., 895 F.3d 1304, 1317–18 (Fed. Cir. 2018) (vacating the jury's monetary award for misappropriation of trade secrets because "evidence supporting [the] claim to monetary relief for trade secret misappropriation did not limit the covered sales to a head-start period, and that omission [could not] be deemed harmless").

63. For example, in *TurnKey Sols. Corp. v. Hewlett Packard Enter. Co.*, No. 15-CV-01541-CMA-CBS, 2017 WL 3425140, at *6–7 (D. Colo. Aug. 9, 2017), the court denied Hewlett Packard's motion for summary judgment limiting TurnKey's damages for trade secret misappropriation and breach of confidentiality agreement to the period prior to the publication of the trade secrets in plaintiff's patent application. In reaching this decision, the court stated: "To the extent HPE is requesting that this Court limit TurnKey's damage award based on the publication of the patent application, the Court declines to do so. The patent application does not necessarily absolve HPE of all post-publication damages that flow from its alleged pre-publication misappropriation." *Id.* Similarly, in *Federal Express Corp. v. Accu-Sort Sys., Inc.*, No. 01-2503 Ma/A, 2005 WL 8156707, at *18 (W.D. Tenn. Mar. 30, 2005), the court denied Accu-Sort's motion for summary judgment seeking a determination "that the time for which FedEx can claim damages ends when FedEx published its patent documents [disclosing] the information at issue in this case." *Id.* at *17. The court recognized generally that "FedEx cannot claim trade secret protection for any information that has been made available to the public by way of a patent," *see id.*, but further recognized that "an act of misappropriation can cause plaintiff to lose profits, or a defendant to receive illicit gains, after the trade secret is made public." *Id.* (collecting cases). "[I]f the 'head start' gained by the defendant through misappropriation continues to disadvantage the

Certain other practical considerations are unique to the head-start approach, including whether the burden of proving the duration of head-start damages falls on the plaintiff (as part of its prima facie case of establishing harm and damages) or the defendant (as an affirmative defense).[64] Courts also consider how the time periods are to be calculated: e.g., based on the head start over the plaintiff's *good-faith competitors* or *the plaintiff itself*, the time it would take defendant to *discover* the trade secret absent misappropriation, or the time necessary to *independently develop* the trade secret into a commercially viable product. And they look at whether the commercial advantage derived from misappropriation should be based on an objective approach that focuses on the actions and capabilities of a good-faith competitor or on a subjective approach that focuses on the actions and capabilities of the misappropriator.

The head-start theory of unjust enrichment damages should not be confused with the test of the same name for determining the accounting period for damages. The latter refers to the "head start" or "lead time" rule, adopted in some jurisdictions, that the damages assessed against a trade secret defendant may be limited to the time it would have taken the defendant to discover the secret without misappropriation or to develop a comparable product without the use of plaintiff's trade secrets.[65] The head-start damages theory awards damages based on a temporal advantage; the head-start accounting period rule imposes a temporal limitation on the amount of damages awarded.

---

plaintiff after the date plaintiff receives its patent, the plaintiff may collect damages for profits that accrue during this 'extra' limited time period." *Id.*

64. *See, e.g.*, *Nite Glow*, at 2021 WL 2945556, at *6–8 ("Determination of head start damages was part of plaintiffs' burden of proof, not an affirmative defense as to which defendants would bear the burden of proof.").

65. Agilent Techs., Inc. v. Kirkland, 2010 WL 610725, at *26 n.230 (Del. Ch. Feb. 18, 2010) (collecting cases).

As a coda on unjust enrichment, New York is the only jurisdiction that does not allow recovery of a defendant's unjust enrichment measured as its avoided development costs—at least where these costs are not used as a proxy for the plaintiff's actual losses. This guidance is premised on a 4–3 decision by the New York Court of Appeals in *E.J. Brooks v. Cambridge Security Seals*, which announced a significant departure from the DTSA and UTSA on unjust enrichment damages.[66] Responding to a question certified to it by the Second Circuit, the Court of Appeals held that under New York common law, a trade secret owner may not recover the development costs the defendant avoided due to its unlawful activity under theories of trade secret theft, unfair competition, or unjust enrichment. In the case of trade secret theft, the court found that damages "must be measured by the losses incurred by the plaintiff," explaining that the avoided cost measure of damages "does not consider the effect of misappropriation on the *plaintiff*. Because this figure is tied to the defendant's gains rather than the plaintiff's losses, it is not a permissible measure of damages."[67]

E.J. Brooks has spawned a number of questions and potential strategies relating to unjust enrichment in New York. To provide a few examples: contrary to some courts and commentators, the holding may not be so broad as to support the interpretation that unjust enrichment is unavailable under New York common law; the case might have been decided differently if the plaintiff had been able to introduce evidence of its own development costs; and the court in *E.J. Brooks* stated that in unfair competition cases "courts may award a defendant's unjust gains as a proxy for compensatory damages," suggesting that evidence of the

66. E.J. Brooks Co. v. Cambridge Security Seals, 31 N.Y.3d 441, 453–56 (N.Y. 2018).

67. *Id.* at 454.

defendant's avoided development costs may be admissible and relevant to measuring the plaintiff's lost profits.[68]

3. Reasonable royalties

a. The availability of reasonable royalty damages varies state to state

Under the language of the UTSA and the DTSA, damages for trade secret misappropriation may be measured by the imposition of liability for a reasonable royalty "[i]n lieu of damages measured by any other methods."[69] Given that the majority of states follow the UTSA on this point without modification, a plaintiff may freely choose in most jurisdictions whether to pursue actual damages or a reasonable royalty damages measure.

Four states—California, Indiana, Georgia, and Illinois—allow a reasonable royalty measure of damages only if other damages are not provable.[70] And Virginia allows reasonable royalty

68. *See id*. at 466; *see also* Tex. Advanced Optoelectronic Sols., Inc. v. Renesas Elecs. Am., Inc., 895 F.3d 1304, 1320 (Fed. Cir. 2018) (the Federal Circuit suggested that evidence of a defendant's gains due to misappropriation might be used as a "case-specific proxy for [plaintiff's] losses or reasonable royalties").

69. Emphasis added. *See* UTSA § 3(a) ("In lieu of damages measured by any other methods, the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret."); *see also* 18 U.S.C. § 1836(b) (same).

70. CAL. CIV. CODE § 3426.3(b); IND. CODE § 24-2-3-4(b); GA. CODE ANN. § 10-1-763(A); 765 ILL. COMP. STAT. ANN. 1065/4(A); *see also, e.g.*, Cacique, Inc. v. Robert Reiser & Co., 169 F.3d 619 (9th Cir. 1999) (applying California law) (holding that royalties cannot be awarded as damages if actual damages or unjust enrichment is provable).

damages only where the plaintiff is "unable to prove a greater amount of damages by other methods of measurement."[71]

Five states—Alaska, Arkansas, Connecticut, Louisiana, and Washington—do not expressly authorize reasonable royalty damages under any circumstances.[72] At least one court has interpreted the lack of an express authorization to mean that reasonable royalty damages are not available.[73] But in the other states, it remains unclear if the lack of express authorization completely forecloses the plaintiff's ability to pursue reasonable royalties when no other remedy is available.

b. Measuring reasonable royalty damages—Two leading methodologies

While the UTSA and DTSA allow for the measurement of trade secret damages using a reasonable royalty in certain circumstances, they do not specify how to measure a reasonable royalty or what constitutes a reasonable royalty under those

71. *See* VA. CODE ANN. § 59.1-338(A). ("Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss. If a complainant is unable to prove a greater amount of damages by other methods of measurement, the damages caused by misappropriation can be measured exclusively by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret.").

72. ALASKA STAT. ANN. § 45.50.915 (West 2007); ARK. CODE ANN. § 4-75-606 (West 2004); CONN. GEN. STAT. ANN. § 35-53 (West 2005); LA. REV. STAT. ANN. § 51:1433 (2003); WASH. REV. CODE ANN. § 19.108.030 (West 2013).

73. *See* Veritas Corp. v. Microsoft Corp., No. 2:06-CV-0703-JCC, 2008 U.S. Dist. LEXIS 112135 (W.D. Wash. Feb. 26, 2008) (denying defendant's motion to exclude testimony of plaintiff's damages expert on the basis that the Washington state statute excludes royalty damages finding defendant's unjust enrichment could be measured by a reasonable royalty).

circumstances.[74] In the absence of guidance, most courts have tended to rely on either *University Computing v. Lykes-Youngstown Corp.*, a leading Fifth Circuit case on pre-UTSA, common law trade secret misappropriation damages, or *Georgia-Pacific Corp. v. U.S. Plywood Corp.*, a leading case on reasonable royalty damages for patent infringement.[75] This section provides an overview of these two methodologies and the issues courts face when applying these approaches.

i. University Computing v. Lykes-Youngstown Corp.

University Computing is a trade secret misappropriation case involving two companies that entered into a joint venture to offer computer services in the southeastern United States.[76] During the formation of the joint venture, the defendants misappropriated a trade secret computerized inventory system from the plaintiff.[77] The defendants intended to sell the system to their own customers but had not sold the system to anyone before

74. *See* Keystone Transp. Sols., LLC v. Nw. Hardwoods, Inc., No. 5:18-cv-00039, 2019 WL 1770162, at *4 (W.D. Va. Apr. 22, 2019) ("The Defend Trade Secrets Act is silent on what qualifies as a 'reasonable royalty' for defendant's use of a misappropriated trade secret" (citation omitted)).

75. Univ. Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 538 (5th Cir. 1974); Georgia-Pacific Corp. v. U.S. Plywood Corp., 318 F. Supp. 1116, 1120 (S.D.N.Y. 1970), *modified by*, Georgia-Pacific Corp. v. U.S. Plywood-Champion Papers, Inc., 446 F.2d 295 (2d. Cir. 1971). *See, e.g.*, Votto v. Am. Car Rental, Inc., No. CV-010456354S, 2003 WL 1477029 (Conn. Super. Ct. 2003) (applying *Georgia-Pacific* factors to trade secret misappropriation), *amended and superseded by* 2003 WL 21716003 (Conn. Super. Ct. 2003), *judgment aff'd*, 871 A.2d 981 (Conn. 2005). *Keystone Transp.*, 2019 WL 1770162, at *4 (recognizing *University Computing* as "a leading case on calculating a reasonable royalty" (citation omitted)).

76. *Univ. Computing*, 504 F.2d at 527.

77. *Id*. at 527–29.

their misappropriation was discovered. Thus, the trial court record did not show any specific loss to the plaintiff or any actual profits by the defendants from their misappropriation.[78]

The Fifth Circuit explained that "the law looks to the time at which the misappropriation occurred to determine what the value of the misappropriated secret would be to a defendant who believes he can utilize it to his advantage, provided he does in fact put the idea to a commercial use."[79] The Fifth Circuit adopted a reasonable royalty measure of damages based on "the fiction that a license was to be granted at the time of beginning the infringement, and them [sic] to determine what the license price should have been."[80] It held that the proper reasonable royalty measure calculates "what the parties would have agreed to as a fair price for licensing the defendant to put the trade secret to the use the defendant intended at the time the misappropriation took place."[81] Evaluating the trial court's jury instructions, the Fifth Circuit affirmed that a willing licensee-willing licensor hypothetical negotiation construct was an accurate statement of the law on reasonable royalty, finding that the jury should determine "what amount would be paid as a reasonable royalty for the unrestricted use of said computer program" by a willing buyer to a willing seller.[82] The Fifth Circuit identified five non-exhaustive factors to consider in a reasonable royalty analysis:

1. the resulting and foreseeable changes in the parties' competitive posture;

---

78. *Id.* at 535–36. Under these circumstances, the parties agreed that the reasonable royalty standard was the appropriate damages measure but were "unable to agree on what the measure entails." *See id.* at 536.

79. *Id.*

80. *Id.* at 537 (quoting Egry Register Co. v. Standard Register Co., 23 F.2d 438, 443 (6th Cir. 1928)).

81. *Id.* at 539.

82. *Id.* at 540.

2. the prices past purchasers or licensees may have paid;
3. the total value of the secret to the plaintiff, including the plaintiff's development costs and the importance of the secret to the plaintiff's business;
4. the nature and extent of the use the defendant intended for the secret; and
5. whatever other unique factors might have affected the parties' agreement, such as the ready availability of alternative processes.[83]

The Fifth Circuit ultimately affirmed the jury award of $220,000 based on expert testimony on the plaintiff's prior offer to sell its trade secrets to a third party for that amount.[84]

University Computing was a leading common law case on trade secret damages when the UTSA's 1985 amendment addressing statutory royalty damages was drafted.[85] Many courts interpreting UTSA-based statutory royalty provisions have either adopted *University Computing*'s five-factor test or have referenced the decision in their analysis.[86]

---

83. *Id*. at 539.

84. *Id*. at 543–46.

85. See Richard F. Dole, Jr., Statutory Royalty Damages Under the Uniform Trade Secrets Act and the Federal Patent Code, 16:2 VAND. J. ENT. & TECH. L. 223, 230–34 (Winter 2014).

86. *See, e.g.*, Steves and Sons, Inc. v. Jeld-Wen, Inc., No. 3:16-CV-545, 2018 WL 2172502, at *7 (E.D. Va. May 10, 2018) ("courts within the Fourth Circuit have turned to *University Computing*, which 'is a leading case on calculating a reasonable royalty'") (citations omitted); Ajaxo Inc. v. E*Trade Fin. Corp., 115 Cal. Rptr. 3d 168, 179–80 (Cal. Ct. App. 2010); Olson v. Nieman's, Ltd., 579 N.W.2d 299, 310–11 (Iowa 1998); Huawei Techs. Co. v. Yiren Huang, No. 4:17-CV-00893, 2019 WL 2395276, at *5 (E.D. Tex. June 6, 2019) (denying motion to strike reasonable royalty expert opinion under *University Computing* where expert relied on two development agreements giving other party access to

As a final note regarding *University Computing*, the Fifth Circuit stated that to be entitled to reasonable royalty damages, the "defendant must have actually put the trade secret to some commercial use."[87] But where the relevant trade secret statute does not require use to find misappropriation, defendants cannot wield *University Computing* to import an otherwise nonexistent commercial use requirement. Courts have been forced to clarify that use is not required to state a claim under the UTSA and the DTSA, emphasizing that improper acquisition alone is sufficient to state a claim for trade secret misappropriation under those statutes.[88] Of course, if improper acquisition alone is sufficient to

---

any and all of defendant's trade secrets); Keystone Transp. Sols., LLC v. Nw. Hardwoods, Inc., No. 5:18-cv-00039, 2019 WL 1770162, at *4 (W.D. Va. Apr. 22, 2019) (approving of expert's "fees-per-container" royalty methodology in DTSA case because it attempts to measure the "actual value of what has been appropriated" under *University Computing*) (quoting *Univ. Computing*, 504 F.2d at 537); *see also* Mid-Michigan Computer Sys., Inc. v. Marc Glassman, Inc., 416 F.3d 505, 510–11 (6th Cir. 2005).

87. *Univ. Computing*, 504 F.2d at 539.

88. Numerous cases have found that misappropriation is properly pleaded under the UTSA and the DTSA based solely on improper acquisition. *See, e.g.*, Source Prod. & Equip. Co. v. Schehr, No. 16-17528, 2017 WL 3721543, at *4 (E.D. La. Aug. 29, 2017) (finding plaintiffs may plead a DTSA misappropriation claim by alleging plausible facts "in support of either the defendants' acquisition or their use of trade secrets"); Brand Energy & Infrastructure Servs., Inc. v. Irex Contracting Grp., No. 16-2499, 2017 WL 1105648, at *3 (E.D. Pa. Mar. 24, 2017) (noting DTSA explicitly contemplates three independent bases for liability, and improper acquisition alone constitutes a misappropriation); Lane v. Brocq, No. 15 C 6177, 2016 WL 1271051, at *13 (N.D. Ill. Mar. 28, 2016) (finding liability under Illinois UTSA attaches for improper acquisition of a trade secret); Williams-Sonoma Direct, Inc. v. Arhaus, LLC, 109 F. Supp. 3d 1009, 1018 (W.D. Tenn. 2015) (finding evidence of acquisition by improper means sufficient under Tennessee UTSA); ATS Prods., Inc. v. Champion Fiberglass, Inc., No. c-13-02403-SI, 2014 WL 466016, at *2 (N.D. Cal. Feb. 3, 2014) (denying motion to dismiss after finding that acquisition, without use, was sufficient to support a misappropriation claim under California UTSA); Hertz v. Luzenac Grp., 576 F.3d 1103, 1115 (10th Cir. 2009) (finding improper

state a claim for trade secret misrepresentation, the next question is whether improper acquisition alone is a sufficient basis for reasonable royalty damages.

When evaluating a royalty, whether fully paid up or on a running royalty basis, the parties will need to consider the useful life and expected future use of the trade secret(s). Reasonable royalties are typically based on the parties' expectations at the time of the hypothetical negotiation, which is generally considered to be on the eve of the misappropriation.

ii. *Georgia-Pacific* 15-factor test

Courts have also used the *Georgia-Pacific* approach to determine reasonable royalty damages in trade secret misappropriation cases, despite the decision primarily addressing patent infringement.[89] Like the *University Computing* court, the court in *Georgia-Pacific* began with a willing licensor-willing licensee construct. The court hypothesized that the plaintiff is a willing licensor negotiating a reasonable royalty license with the defendant,

---

acquisition of trade secret alone sufficient under Colorado UTSA); Semper/Exeter Paper Co. v. Henderson Specialty Paper LLC., No. SACV 09-0672 AG (MLGx), 2009 WL 10670619, at *5 (C.D. Cal. Sept. 21, 2009) (finding "improper acquisition" alone sufficient to state a claim where former employee sent trade secrets from his work email to a personal email) (quoting San Jose Const., Inc. v. S.B.C.C., Inc., 155 Cal. App. 4th 1528, 1544 (Cal. Ct. App. 2007) ("[U]nder the UTSA 'misappropriation' can occur through improper *acquisition* of a trade secret, not only through use."); Dealertrack, Inc. v. Huber, 460 F. Supp. 2d 1177, 1184 (C.D. Cal. 2006) (denying motion to dismiss California UTSA claim for failing to plead use of trade secrets because plaintiffs properly pleaded improper acquisition). The question of what remedy can be afforded for acquisition liability remains a subject for discussion.

89. *See, e.g.*, O2 Micro Int'l Ltd. v. Monolithic Power Sys., Inc., 399 F. Supp. 2d 1064, 1078 (N.D. Cal. 2005), *amended on other grounds*, 420 F. Supp. 2d 1070 (N.D. Cal. 2006), *aff'd per curiam*, 221 F. App'x 996 (Fed. Cir. 2007) (unpublished decision); LinkCo, Inc. v. Fujitsu Ltd., 232 F. Supp. 2d 182, 186 n.7 (S.D.N.Y. 2002).

who is a willing licensee, at the time the infringement began — a construct referred to as the "hypothetical negotiation[ ]."[90] To determine the reasonable royalty that would result from the hypothetical negotiation, the *Georgia-Pacific* court identified 15 categories of evidence to consider.[91]

The many significant differences between patents and trade secrets mean that the *Georgia-Pacific* factors should not simply be imported into trade secret misappropriation cases without thoughtful consideration. For example, many of the *Georgia-Pacific* factors are based on benchmark licenses or royalties for the technology (e.g., factors 1, 2, 3, and 4) that are highly unlikely to exist in trade secret cases where the value of the trade secret depends on keeping it a secret. Moreover, many other *Georgia-Pacific* factors (e.g., factors 6, 8, and 10) are traditionally analyzed through sales of commercialized products; yet if the parties are engaging in a reasonable royalty analysis because actual loss and unjust enrichment are not provable, it may be because the trade secret misappropriation occurred in a nascent market that, by definition, does not have commercialized products. Additionally, some argue that the entire construct of a hypothetical negotiation to license one's most fiercely guarded trade secrets to a competitor is inconsistent with the whole point of having trade secrets. Thus, finding appropriate data points to inform such a negotiation can be especially challenging in a trade secret case.[92]

---

90. Georgia-Pacific Corp. v. U.S. Plywood Corp., 318 F. Supp. 1116, 1120–22 (S.D.N.Y. 1970).

91. *Id.* at 1120.

92. An analysis of trade secret damages awards supports this reasoning—just under five percent of damages awards for trade secrets claims were for a reasonable royalty from 2000 to 2014. Elizabeth A. Rowe, *Unpacking Trade Secret Damages*, 55 HOUS. L. REV. 155, 175 (2017). The vast majority of damages awarded in trade secrets cases are for compensatory damages, including lost profits and unjust enrichment. *Id.* ("Approximately 85% of the awards consisted of compensatory damages.").

In many instances, this problem is exacerbated when courts must turn to the reasonable royalty measure as the damages measure of last resort when actual loss and unjust enrichment fail to provide a nonspeculative measure.

C. Speculation and Reasonable Certainty

Principle No. 2 – The existence of damages and the measurement of a monetary damages award for misappropriation must not be speculative, but the amount of damages need not be proved with mathematical certainty.

Once the fact of misappropriation is proved, trade secret cases have expressly relaxed the level of certainty required to measure the amount of money to award as damages.[93] The law requires only that some reasonable basis for computing damages be used, and that damages may be computed even if the result reached is an approximation.[94] Illustrative are the jury instructions in recent trade secret trials that the amount of damages did

93. *See, e.g.*, Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc., 35 F.3d 1226, 1245 (8th Cir. 1994) ("If it is speculative and uncertain whether [trade secret] damages have been sustained, recovery is denied. [But] [i]f the uncertainty lies only in the amount of damages, recovery may be had if there is proof of a reasonable basis from which the amount can be inferred or approximated." (citations omitted)); Stanacard, LLC v. Rubard LLC, 12 Civ. 5176 (CM), 2016 WL 6820741, at *4 (S.D.N.Y. Nov. 10, 2016); Weston v. Buckley, 677 N.E.2d 1089, 1093 (Ind. Ct. App. 1997) ("Although [a damages award for trade secret misappropriation] cannot be based upon mere speculation or guesswork, no degree of mathematical certainty is required in the damage calculation." (citation omitted)).

94. *See, e.g.*, Sargon Enters., Inc. v. Univ. of S. Cal., 55 Cal. 4th 747, 774 (Cal. 2012); Meister v. Mensinger, 230 Cal. App. 4th 381, 396–97 (Cal. Ct. App. 2014); Leoni v. Bemis Co., 255 N.W.2d 824, 825 (Minn. 1977); Storage Tech. Corp. v. Cisco Sys., Inc., 395 F.3d 921, 928–29 (8th Cir. 2005).

not need to be shown with "mathematical precision," so long as the jurors did not "speculate or guess in awarding damages."[95]

A general rule in most jurisdictions is that if damages are difficult to establish, an injured party need only prove damages with reasonable certainty.[96] For example, in *Stanacard, LLC v. Rubard LLC*, the court stated that: "The rule which proscribes the recovery of uncertain and speculative damages applies where the fact of damages is uncertain, not where the amount is uncertain . . . . Damages are not rendered uncertain because they cannot be calculated with absolute exactness . . . . Their extent may be established 'as a matter of just and reasonable inference, although the result be only approximate.'"[97]

D. Theories of Monetary Relief in Trade Secret Cases May Overlap, But No Double Counting is Permitted

Principle No. 3 – Multiple theories of measuring damages for misappropriation may be applied so long as there is no double counting.

As long as there is no double counting, damages for trade secret misappropriation can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss.[98]

---

95. Jury Instructions at 37, Steves and Sons, Inc. v. Jeld-Wen, Inc., No. 3:16-CV-545, 2018 WL 2172502 (E.D. Va. May 10, 2018) D.I. 1614 (verdict for plaintiff); Final Jury Instructions at 41–42, BladeRoom Grp. Ltd. v. Facebook, Inc., 2018 WL 1611835 (N.D. Cal. May 7, 2018) D.I. 827-1 (same).

96. Spector v. Fireman's Fund Ins. Co., 451 Fed. App'x 130, 134 (3d Cir. 2011) (quoting ATACS Corp. v. Trans World Commc'ns, Inc., 155 F.3d 659, 669–70 (3d Cir. 1998)).

97. *Stanacard*, 2016 WL 6820741 at *4; *See also Weston*, 677 N.E.2d at 1093.

98. UTSA With 1985 Amendments § 3(a) and related comments ("Damages can include both the actual loss caused by misappropriation and the unjust

For example, when both lost profits and unjust enrichment damages are claimed, it is important to address the extent to which there is overlap between these damage claims. In those instances where there is complete overlap, basing an award on the higher amount can typically eliminate any double counting. However, in situations where there is partial overlap between different damages measures, it is important that there be sufficient detail and information providing a basis for elimination of any potential double counting.

E. Additional Issues

In addition to the core principles described above, other issues repeatedly arise when assessing damages in trade secret cases. This section addresses several such issues, including timing, causation, apportionment, and the interplay between monetary remedies for trade secret misappropriation and other legal theories and equitable remedies.

1. Timing

<u>Guideline No. 1</u> – The duration of the trade secret damages period should align with the elimination of defendant's unfair commercial advantage.

In defining a damages period, it is widely recognized that trade secret damages are recoverable for the period of time necessary to eliminate the unfair commercial advantage gained

---

enrichment caused by misappropriation that is not taken into account in computing actual loss." "As long as there is no double counting, Section 3(a) adopts the principle of the recent cases allowing recovery of both a complainant's actual losses and a misappropriator's unjust benefit that are caused by misappropriation.").

from actionable misappropriation.[99] This concept, well grounded in UTSA principles and related commentary, is sometimes described as the "head start rule" or as extending damages as long as necessary to remedy a "head start or other unfair advantage."[100]

The secrecy period is the time the trade secrets were unknown or not ascertainable through proper means. One can be liable for trade secret misappropriation only if the misappropriation takes place during this secrecy period.[101] The duration of the damages period for trade secret misappropriation, however, may extend beyond the secrecy period as necessary to eliminate

---

99. The UTSA does not expressly limit the time for calculating money damages. However, the comments to Section 3 of the UTSA, which permits monetary damages, adopts the time limits stated in Section 2, which permits injunctive relief. UTSA § 3 cmt. ("Like injunctive relief, a monetary recovery for trade secret misappropriation is appropriate only for the period in which information is entitled to protection as a trade secret, plus the additional period, if any, in which a misappropriator retains an advantage over good faith competitors because of misappropriation."). *See also id.*, § 2(a) ("[An] injunction may be continued for an additional reasonable period of time in order to eliminate commercial advantage that otherwise would be derived from the misappropriation.").

100. RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 45 cmt. h (AM. LAW INST. 1995) (extending monetary relief "to the extent necessary to remedy a head start or other unfair advantage attributable to defendant's prior access to information").

101. A court may determine the secrecy period would have ended earlier than the rest of the market would otherwise have ascertained the trade secret if the court finds the defendant would have independently ascertained the trade secret earlier than that. *See, e.g.*, Agilent Techs. v. Kirkland, 2010 WL 610725 (Del. Ch. Feb. 18, 2010) (awarding lost profits and unjust enrichment damages for a three-year period representing the time it would have taken defendant to develop commercially viable and competitive product absent the unauthorized use of plaintiff's trade secrets, plus an additional year of lost-profit damages beyond the head-start period to address defendant's increased market share).

any unfair commercial advantage or other financial impact due to the trade secret misappropriation.[102] Courts have rejected efforts by defendants to limit damages to the head start gained in their development of a competing product where this excludes or could exclude the plaintiff's recovery for other losses or other ways the defendant has been unjustly enriched.[103]

---

102. *See e.g.*, Federal Express Corp. v. Accu-Sort Sys., Inc., No. 01-2503 Ma/A, 2005 WL 8156707, at *17–18 (W.D. Tenn. Mar. 30, 2005) (denying motion for summary judgment seeking to cut off damages as of issuance of patent and stating, "an act of misappropriation can cause plaintiff to lose profits, or a defendant to receive illicit gains, after the trade secret is made public . . . . Whether and to what extent any such damages may be measured by profits Accu-Sort made after FedEx sought or received its patents remains a disputed question of fact."); *see also* TurnKey Sols. Corp. v. Hewlett Packard Enter. Co., No. 15-cv-01541-CMA-CBS, 2017 WL 3425140, at *6 (D. Colo. Aug. 9, 2017) (denying Hewlett Packard's motion for summary judgment limiting TurnKey's damages for trade secret misappropriation and breach of confidentiality agreement to the period prior to the publication of the trade secrets in plaintiff's patent application).

103. Johns Manville Corp. v. Knauf Insulation, LLC, No. 15-CV-00531-RBJ-KLM, 2017 WL 4222621, at *8–10 (D. Colo. Sept. 22, 2017) (denying defendant's motion for summary judgment seeking to limit plaintiff's damages to the head-start period); Sabre GLBL, Inc. v. Shan, 779 Fed. App'x 843, 851 (3d Cir. 2019) (rejecting challenge to arbitrator's award of head-start damages based on lack of evidence of saved development costs because head-start damages and saved development costs are not "the same thing"); Alifax Holding SpA v. Alcor Sci. Inc., 404 F. Supp. 3d 552, 573 (D.R.I. 2019) (head-start damages was one of two alternative approaches for calculating unjust enrichment damages); *Agilent Techs.*, 2010 WL 610725, at *27 (to prevent what the court deemed "underenforcement" and in order to avoid having to enter an injunction enjoining sales of the defendant's competing product, the court awarded an additional year of actual loss damages beyond the head-start period).

2. Causation

Guideline No. 2 – A trade secret plaintiff bears the burden to prove that defendant's misappropriation was the proximate cause of its damages.

A plaintiff alleging misappropriation of trade secrets must prove proximate causation to receive damages for its lost sales, its lost profits, or disgorgement of a defendant's profits.[104] The plaintiff also bears the burden to prove causation of its own losses (whether sales or profits).[105]

---

104. *See* 18 U.S.C. § 1836(b)(3)(B)(i) (authorizing award for "actual loss caused by the misappropriation" and disgorgement of "any unjust enrichment caused by the misappropriation"); UTSA With 1985 Amendments § 3 (same); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 45 (AM. LAW INST. 1995) (plaintiff may seek monetary relief for "pecuniary loss . . . caused by" misappropriation or "pecuniary gain resulting from" misappropriation).

105. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 45 cmt. b (AM. LAW INST. 1995) ("The plaintiff bears the burden of proving the fact and cause of any loss for which recovery is sought"); *see also*, *e.g.*, *In re* TXCO Res., Inc., 475 B.R. 781, 822–23 (Bankr. W.D. Tex. 2012) (applying Texas law: "In order to recover actual damages, [aggrieved party] was first required to show that [alleged misappropriator's] use of [aggrieved party's] trade secrets proximately caused [it] to suffer a specific injury"); Scentsational Techs., LLC v. Pepsico, Inc., No. 13-CV-8645 (KBF), 2018 WL 2465370, at *7 (S.D.N.Y. May 23, 2018), *aff'd*, 773 F. App'x 607 (Fed. Cir. 2019) ("[I]n order to hold a party liable for lost profits [due to misappropriation], a plaintiff must establish proximate causation by the defendant."); Firetrace USA., LLC v. Jesclard, 800 F. Supp. 2d 1042, 1055 (D. Ariz. 2010) (summary judgment appropriate where plaintiff failed to show disclosure or use was "substantial factor" in development of competing product); Hunter Bldgs. & Mfg., L.P. v. MBI Glob., L.L.C., 436 S.W.3d 9, 18 (Tex. App. 2014) ("To recover lost profits, the plaintiff must produce evidence from which the jury reasonably may infer that the lost-profits damages for which recovery is sought have resulted from the conduct of the defendant.").

Regarding disgorgement, a plaintiff generally must show that the defendant's misappropriation proximately caused the defendant's unjust enrichment.[106] After that showing, the burden then shifts to the defendant to apportion the value of the defendant's profits or other benefit attributable to its wrongdoing.[107] Notwithstanding any burden shifting, then, the ultimate proof of proximate causation regarding disgorgement of a defendant's profits or unjust benefits will likely remain the responsibility of the plaintiff.

On the other hand, courts have generally not required plaintiffs to show proximate causation before awarding reasonable royalties.[108] Some states, such as California and Delaware, explicitly provide that reasonable royalties may be available in the

106. *See, e.g.*, Propulsion Techs., Inc. v. Attwood Corp., 369 F.3d 896, 905 (5th Cir. 2004) (finding judgment as a matter of law appropriate where "there is no evidence that [defendant] used trade secrets to generate [its] profits"); GeoMetWatch Corp. v. Hall, No. 1:14-CV-60-JNP, 2018 WL 6240991 at *15 (D. Utah Nov. 27, 2018) (granting summary judgment against unjust enrichment theory under Utah Uniform Trade Secrets Act for plaintiff's failure to show defendants were enriched by "sales attributable to the use of the trade secret"); *In re* Nortel Networks, Inc., No. 09-10138(KG), 2016 WL 491639, at *9 (Bankr. D. Del. Feb. 8, 2016) ("The plaintiff bears the burden of demonstrating that defendant's misappropriation proximately caused its unjust enrichment.") (citing Total Care Physicians, P.A. v. O'Hara, No. Civ.A. 99C-11-201JRS, 2003 WL 21733023, at *2 (Del. Super. July 10, 2003)).

107. *See* Univ. Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 539 (5th Cir. 1974) ("If the defendant enjoyed actual profits, a type of restitutionary remedy can be afforded the plaintiff—either recovering the full total of defendant's profits or some apportioned amount designed to correspond to the actual contribution the plaintiff's trade secret made to the defendant's commercial success.").

108. *See* 18 U.S.C. § 1836(b)(3)(B)(ii) ("in lieu of damages measured by other methods, the damages caused by the misappropriation [may be] measured by imposition of liability for a reasonable royalty for the misappropriator's unauthorized disclosure or use of the trade secret"); UTSA With 1985 Amendments § 3 (same).

absence of proof of actual damages or disgorgement.[109] A reasonable royalty, however, "attempts to measure the value to the defendant to what he appropriated," even where no profit was realized as a counterfactual "reasonable estimate of value" of the trade secret.[110] It is thus not generally subjected to proof of proximate cause.[111] Nevertheless, as the value of a reasonable royalty is generally tied (at least in part) to the scope of the misappropriation, facts relating to proximate causation should remain relevant to the determination of a reasonable royalty.[112]

---

109. *See, e.g.*, CAL. CIV. CODE § 3426.3(b) ("If neither damages nor unjust enrichment caused by misappropriation are provable, the court may order payment of a reasonable royalty for no longer than the period of time the use could have been prohibited."); DEL. CODE ANN. tit. 6, § 2003 ("In lieu of damages measured [by actual loss or unjust enrichment], the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty").

110. *Univ. Computing*, 504 F.2d at 537–38.

111. *See, e.g.*, *In re* TXCO Res., Inc., 475 B.R. 781, 825 (Bankr. W.D. Tex. 2012) ("As opposed to an award of damages for lost profits, which requires the plaintiff to prove proximate causation and damages with reasonable certainty, an award of damages based on a reasonable royalty does not require the plaintiff to prove a specific injury."); Atl. Inertial Sys. v. Condor Pac. Indus. of Cal., No. 2:08-CV-02947-CAS, 2015 WL 3825318, at *7 (C.D. Cal. June 18, 2015) (rejecting defendant's argument that reasonable royalty could not be awarded where there was no proof of proximate cause); DiscoverOrg Data, LLC v. Bitnine Glob., Inc., No. 19-CV-08098-LHK, 2020 WL 6562333, at *9 (N.D. Cal. Nov. 9, 2020) (awarding reasonable royalty despite admitted lack of evidence of proximate cause).

112. *See, e.g.*, *Atl. Inertial Sys.*, 2015 WL 3825318, at *6 (factor in determining value of reasonable royalty under California law includes "whether some benefit, pecuniary or otherwise, accrued to the misappropriating defendant"); *In re TXCO*, 475 B.R. at 826 (factor in determining value of reasonable royalty under Texas law includes "the nature and extent of the use the defendant intended for the secret").

3. Apportionment

<u>Guideline No. 3</u> – In cases where multiple trade secrets are asserted, the trade secret claimant should provide evidence of apportionment of damages or evidence why an apportionment is not appropriate.

A related issue to causation is "apportionment"—that is, to focus the damages on scope of the relevant trade secrets and not anything else. Apportionment in trade secret damages refers to two issues. First, the product or service in question may or may not have parts or components unrelated to the trade secrets. If so, an evaluation should be done as to the trade secrets' "integral nature" in the product, and their contributions to total product value. Second, if there are multiple trade secrets, an additional evaluation should be done as to different trade secrets' contributions to value, if they are separable.

a. Product Value Apportionment

Where the product or service accused of incorporating misappropriated trade secrets is complex enough to have several constituent parts, only some of which contain one or more trade secrets, the valuation question arises as to the relative importance, or contribution, of the trade secrets to the value of the whole product or service. This question is specific to the scope of the trade secrets and the nature of the accused product or service.

It may be that the entire value of the product is fairly attributed to the trade secrets because they are the primary driver of the demand for the product. Often, though, there are multiple drivers of demand, especially for complex products. Techniques

of demand-side analysis[113] exist that may shed light on the question of the relative contribution of the trade secrets to the total value of the product. If the trade secrets do not easily map to product features visible to the customer, it may be that they contribute value by reducing costs an identifiable amount, thereby contributing to incremental profit. Through all these types of analysis, it is important to avoid ad hoc techniques and to tie the chosen methods closely to the facts of the trade secrets and products in the case. For example, the court in *Waymo v. Uber* criticized Waymo's expert's reliance on the Uber document concerning incremental profits because there was "no apportionment for the *legitimate* elements of the Ottomotto acquisition."[114] The Southern District of New York reached a similar requirement in *In re Avaya, Inc.*, holding that apportionment is required where a product includes both legitimately acquired benefits and misappropriated trade secrets.[115] The *Avaya* court borrowed heavily from patent law in its ruling that apportioning the value of a trade secret based on "the cost or price of a component compared

113. Two such examples are hedonic feature regressions, which explore the degree to which external and internal factors affect demand, and conjoint customer surveys, a research technique used to quantify values of individual features of a product or service.

114. Waymo LLC v. Uber Techs., Inc., No. C-17-00939-WHA, 2017 WL 5148390, at *4, *6 (N.D. Cal. Nov. 6, 2017). *See also* StoneCoat of Texas, LLC v. ProCal Stone Design, LLC, 426 F. Supp. 3d 311, 352 (E.D. Tex. 2019) ("Plaintiffs have not presented evidence that provides any means of distinguishing revenue [defendants] gained from other sources from revenue gained through misappropriation of [the trade secrets], let alone a calculation of profits from the relevant portion of revenue." (citation omitted)).

115. *In re* Avaya Inc., No. 17-10089 (SMB), 2018 WL 1940381, at *8 (Bankr. S.D.N.Y. Apr. 23, 2018), *aff'd,* 602 B.R. 445 (S.D.N.Y. May 6, 2019).

to the cost of the entire multi-component product" was appropriate.[116]

b. Multiple Trade Secret Apportionment

Where multiple trade secrets are asserted, one should assess apportionment of damages among the various claimed trade secrets. While trade secret law remains unsettled regarding whether apportionment is required, courts are increasingly likely to require some element of apportionment. The likelihood that apportionment will be required increases when the trade secret plaintiff asserts larger numbers of trade secrets or the accused product/service at issue is a composite of accused and nonaccused components. Upon investigation, it may be the case that each asserted trade secret is so integral to the product that it is truly impossible to apportion value between them.[117] It may also be the case that each trade secret, or subsets of the asserted trade secrets, overlap in their contribution to product value, such that the total damages amount results as long as the jury finds liability for at least one, or one group, of the trade secrets. Or, as the *LivePerson v. [24]7.AI*[118] case (below) illustrates, it may be possible to parse out what parts of damages result from the infringement of certain trade secrets, such that adding up the parts generates the total damages should the jury find liability for all the asserted trade secrets.

---

116. *Id.*, at *8–9 ("Arnold properly measured the unjust enrichment by apportioning the value of the trade secrets to the entire PSU based on the cost of their components.").

117. *See, e.g.*, Huawei Techs. Co. v. Yiren Huang, No. 4:17-CV-00893, 2019 WL 2395276, at *3 (E.D. Tex. June 6, 2019) ("[Plaintiff] is a small start-up company . . . the asserted trade secrets are an integral part of the . . . research and development and it is not possible to identify and apportion research and development expenses that are tied solely to the ten trade secrets.").

118. No. 17-CV-01268-JST, 2018 WL 6257460 (N.D. Cal. Nov. 30, 2018).

The following representative opinions illustrate some instances where the courts have emphasized the importance of addressing multiple trade secret apportionment as part of their damages analysis.

In *O2 Micro International v. Monolithic Power Systems*, the plaintiff alleged eleven trade secrets were misappropriated, but the jury found only five of the trade secrets were misappropriated, and only one misappropriated trade secret resulted in the defendant being unjustly enriched.[119] Since the plaintiff's damages expert "provided the jury with a damages calculation based on an assumption that all of the trade secrets were misappropriated," the jury was "then left without sufficient evidence, or a reasonable basis, to determine the unjust enrichment damages."[120] As a result, the court vacated the jury's award of $12 million unjust enrichment damages for the misappropriation of trade secrets on the grounds that the plaintiff failed to prove unjust enrichment damages for the trade secrets that the jury found to have been misappropriated.[121]

Following the practical logic in *O2 Micro*, courts frequently require apportionment of damages among individual trade secrets.[122] For example, in *LivePerson,* the court excluded a damages expert's opinion "because he does not apportion trade secret misappropriation damages among particular alleged trade secrets, and offers no methodology for the jury to calculate trade secret misappropriation damages on fewer than all of the 28

119. 399 F. Supp. 2d 1064, 1076–77 (N.D. Cal. 2005).

120. *Id*.

121. *Id*. at 1077.

122. *See, e.g.*, Tex. Advanced Optoelectronic Sols., Inc. v. Renesas Elecs. Am., Inc., 895 F.3d 1304, 1317 (Fed. Cir. 2018), *cert. denied*, 139 S.Ct. 2741 (2019); Ford Motor Co. v. Versata Software, Inc., No. 15-11624, 2018 WL 10733561, at *10–11 (E.D. Mich. July 9, 2018).

alleged trade secrets in the case."[123] The plaintiff's expert addressed the court's concerns in a supplemental report, apportioning the trade secrets by (1) apportioning damages by customers with whom the trade secret was associated, (2) apportioning damages to three categories of trade secrets, and (3) apportioning damages within those categories.[124] The court accepted the new apportionment despite the defendant's concerns about using a "per-unit calculation."[125]

But apportionment may not be required if the facts suggest otherwise. For example, in *BladeRoom Group v. Emerson Electric*, the jury awarded the plaintiff $10 million in lost profit damages and $20 million in unjust enrichment damages for the defendant's misappropriation of the plaintiff's trade secrets.[126] Posttrial, the defendant challenged the sufficiency of the evidence to support the damages award, in part because "the jury was not asked to apportion damages among the trade secrets."[127] The court rejected the defendant's argument and upheld the damages awards, stating: "Relevant California authority does *not* require an apportionment of damages."[128] The court reasoned that in the absence of a rule requiring apportionment, the plaintiff "could argue that since its trade secrets encompass the designs and methods used to create parts of a unified structure, the misappropriation of any of the asserted trade secrets would have caused all of the damages it sought."[129]

---

123. 2018 WL 6257460, at *2.

124. *Id.* at *2.

125. *Id*. at *3–4.

126. 331 F. Supp. 3d 977, 979 (N.D. Cal. 2018).

127. *Id*. at 989.

128. *Id.* (emphasis added).

129. *Id.*; *see also* Sabre GLBL, Inc. v. Shan, 779 Fed. App'x 843, 852 (3d Cir. 2019); CardiAQ Valve Techs., Inc. v. Neovasc Inc., No. 14-CV-12405-ADB, 2016 WL 6465411, at *11–12 (D. Mass. Oct. 31, 2016) (denying motion for new

Similarly, in *Huawei Technologies v. Yiren Huang*, the court permitted the plaintiff's expert to testify that it was not possible to apportion damages by trade secret because the trade secrets were all integral to the product.[130] The court reasoned that "failure to apportion is not fatal" to the expert's opinion because whether the full amount of damages is attributable to the misappropriation of trade secrets is for the jury to decide.[131] Accordingly, "any challenges to that model and allocation scheduled set forth in the [Expert] Report is best handled on cross-examination."[132]

4. Interplay between monetary remedies for misappropriation of trade secrets and other legal theories, including breach of contract

<u>Guideline No. 4</u> – Claims for trade secret misappropriation and for misuse of confidential information in breach of contractual obligations are not necessarily interchangeable. Liability and remedies under each theory should be analyzed separately.

The UTSA "displaces conflicting tort, restitutionary, and other . . . civil remedies for misappropriation of a trade secret,"[133] but "does not affect: (1) contractual remedies, whether or not

---

trial on damages where jury found three of six asserted trade secrets misappropriated and expert did not testify as to reasonable royalty for each trade secret because court found jury had reasonable basis to conclude that the individual trade secrets misappropriated solved the same challenges and gave defendant the same head start).

130. 2019 WL 2395276, at *3 (E.D. Tex. June 6, 2019).

131. *Id.* at *4.

132. *Id*.

133. UTSA § 7(a).

based upon misappropriation of a trade secret." [134] The DTSA does not "preempt or displace any other remedies."[135] Accordingly, actions for breach of contract are consistent with both trade secret statutes. In fact, many trade secret cases include claims seeking monetary damages for breach of confidentiality or nondisclosure agreements by former employees or business partners. In reviewing these claims, courts undertake as a separate inquiry the interpretation and enforceability of these contracts.

The elements of liability and remedies for a breach of contract or other asserted claims do not mirror the elements of liability and remedies for misappropriation of trade secrets. For example, while protectable trade secrets require proof of reasonable efforts by the owner to maintain secrecy and that the information to be protected derives independent economic value from having been kept secret, a contractual obligation of confidentiality is not necessarily tethered to the same requirements.[136] In addition, the timeliness of a contract claim is often based on the accrual of the cause of action, i.e., as of the date of breach, while the timeliness of a misappropriation claim is based on the date the trade secret owner discovered (or reasonably should have discovered) the misappropriation.[137] Remedies differ in many aspects as

---

134. UTSA § 7(b).

135. 18 U.S.C. § 1838.

136. *See, e.g.*, FLA. STAT. § 542.335 (in the course of defining "legitimate business interests" that may be protected in written restrictive covenant, this Florida statute expressly differentiates "trade secrets" from "valuable confidential or business information that otherwise does not qualify as trade secrets" (emphasis added)).

137. *See* Ocimum Biosolutions (India) Ltd. v. AstraZeneca UK Ltd., No. N15C-08-168-AML-CCLD, 2019 WL 6726836, at *8 (Del. Super. Ct. Dec. 4, 2019) (the statute of limitations for breach of contract begins to run "at the time of the wrongful act" (the accrual of the cause of action); in comparison, the statute of limitations for trade secret misappropriation under Delaware's

well, including that punitive damages generally are not available for breach of contract but are available for willful trade secret misappropriation.[138] In short, breach of contract claims have different elements and damage theories from statutory trade secret claims; a success on one group of claims is no guarantee of success on the other.[139]

In addition, the resolution of contractual or other legal claims, on the one hand, and trade secret claims on the other, may influence the resolution of each other in particular disputes.[140] For example, a nondisclosure agreement may define and give notice of the trade secrets being protected, and may set a time limit during which information designated under the agreement is deemed confidential. The danger to the trade secret holder is that a failure to include material could be argued as a waiver, and a contractually set time limit—which may have been set before the parameters of the trade secret were fully understood—may then be determinative on the duration of trade secret protection under the law.[141] For another example, if the trade

---

UTSA "begins to run after the misappropriation is discovered or by the exercise of reasonable diligence should have been discovered." (citations omitted)).

138. UTSA § 3(b).

139. *E.g.*, AcryliConUSA, LLC v. Silikal GmbH, 985 F.3d 1350 (11th Cir. 2021); OrthoFix, Inc. v. Hunter, 630 F. App'x 566 (6th Cir. 2015); Whiteslate, LLP v. Dahlin, 20-CV-1782 W (BGS), 2021 WL 2826088 (S.D. Cal. July 7, 2021).

140. *See, e.g.*, BladeRoom Group Ltd v Emerson Electric Co., 11 F.4th 1010, 1017, 1022–24 (9th Cir. 2021) (holding that district court erred in interpreting Emerson's confidentiality obligations under the nondisclosure agreement and thus vacated the jury's findings not just on breach of contract, but also its findings on misappropriation of trade secrets, its award of damages for breach of contract and trade secret misappropriation, and its determination that defendant willfully and maliciously misappropriated plaintiff's trade secrets (for which the district court awarded punitive damages)).

141. *See, e.g.*, Silicon Image, Inc. v. Analogix Semiconductor, Inc., No. C-07-00635 JCS, 2008 WL 166950, at *8, *16–17 (N.D. Cal. Jan. 17, 2008); On-Line

secret holders fail to comply with the confidentiality requirements specified in the nondisclosure agreement, a waiver may be found (or at least claimed).[142]

5. Interplay between monetary remedies and equitable remedies in trade secret cases

Guideline No. 5 – From the outset of a case, the parties should consider all available equitable and monetary remedies, since the parties' positions on equitable remedies will affect their positions on monetary remedies and vice versa.[143]

Under the appropriate circumstances, courts are empowered to grant both damages and injunctive relief.[144] Given the facts of a particular case, the parties and the court should consider how the approach to monetary relief may affect the entitlement to injunctive relief and vice versa.[145]

To obtain interim or permanent injunctive relief, the moving party must establish that, absent relief, it will suffer irreparable harm. As part of this assessment, courts focus on whether

---

Techs. v. Perkin Elmer Corp., 141 F. Supp. 2d 246, 256 (D. Conn. 2001); DB Riley, Inc. v. AB Engineering Corp., 977 F. Supp 84, 91 (D. Mass. 1997); ECT Int'l, Inc. v. Zwerlein, 597 N.W.2d 479, 484–85 (Wis. Ct. App. 1999).

142. *See, e.g.*, Convolve, Inc. v. Compaq Computer Corp., 527 F. App'x 910, 925 (Fed. Cir. 2013).

143. *See also* The Sedona Conference, *Commentary on Equitable Remedies in Trade Secret Litigation*, Guideline 13, 23 SEDONA CONF. J. 591, 721 (2022) [hereinafter *Sedona Trade Secret Equitable Remedies*].

144. Steves & Sons, Inc. v. Jeld-Wen, Inc., No. 3:16-CV-545, 2018 WL 6272893, at *4 (E.D. Va. Nov. 30, 2018) (interpreting DTSA and Texas UTSA and collecting cases).

145. Whether injunctive relief is available to remedy trade secret misappropriation and, if so, in what form is discussed in in *Sedona Trade Secret Equitable Remedies*, *supra* note 143.

monetary relief is possible to quantify under the circumstances and if it will make the movant whole, such that the movant has an "adequate remedy at law" and therefore is not entitled to injunctive relief.[146]

Movants often cite the loss of business goodwill or threats to established customer relationships as circumstances that are difficult if not impossible to compensate with money damages, but they must show these claims to be true, not just recite conclusory or speculative allegations.[147]

---

146. DVD Copy Control Assn., Inc. v. Kaleidescape, Inc., 176 Cal. App. 4th 697, 702, 726 (Cal. Ct. App. 2009); *See, e.g.*, Bladeroom Grp. Ltd. v. Emerson Elec. Co., No. 5:15-cv-01370-EJD, 2019 WL 1117537, at *2 (N.D. Cal. Mar. 11, 2019) ("In other words, to say that the harm is irreparable is simply another way of saying that pecuniary compensation would not afford adequate relief or that it would be extremely difficult to ascertain the amount that would afford appropriate relief") (*citing DVD Copy Control*, 176 Cal. App. 4th at 722), *rev'd on other grounds, vacated judgment and post-verdict orders and remanded for new trial on breach of contract, misappropriation and damages, and vacated award of attorneys' and expert witness fees by*, 11 F.4th 1010, 1022, 1024 (9th Cir. 2021).

147. *See generally* the discussion in the *Sedona Trade Secret Equitable Remedies*, *supra* note 143, at 694 n.194 (*citing In re* Document Techs. Litig., 275 F. Supp. 3d 454, 469 (S.D.N.Y. 2017) (rejecting "conclusory statements from [plaintiff's] Chief Integration Officer that the company saw 'harm to [its] good will' because of the defendant's 'abrupt' departure," finding that it is precisely such 'unsubstantiated testimony, disconnected from proof that any customers have actually ceased doing business with [plaintiff] or testimony from any clients that they think less of the company, that New York courts have held is insufficient to show actual or imminent harm to a plaintiff's "goodwill"); Katch, LLC v. Sweetser, 143 F. Supp. 3d 854, 875 (D. Minn. 2015) (finding that plaintiff had offered no explanation as to why damages would be impossible to measure or any more difficult than any other situation in which a party claims damages based on lost profits); Rapco Foam, Inc. v. Sci. Applications, Inc., 479 F. Supp. 1027, 1031 (S.D.N.Y. 1979) (finding that claiming there would be a "loss of competitive advantage" absent relief was not in itself sufficient to warrant injunctive relief where plaintiff presented no evidence concerning its position in the marketplace, the nature of competition within that market, or the impact of the misappropriation sufficient to show that any loss

Enlisting economic experts at an early stage to assist the court in deciding a motion for interim injunctive relief can cut both ways. Depending on the nature of the alleged trade secrets and their misappropriation, the proffered testimony may show either the futility of attempting to measure money damages or the likelihood of developing a plausible claim for money damages.[148]

Where damages awarded at the end of a case compensate a forward-looking injury, courts will often deny the request for injunctive relief as duplicative of the monetary relief, even if the damages award is less than the movant requested.[149] Where, however, the damages award is found to compensate for past harm, it may be appropriate to enter a forward-looking permanent injunction to prevent the future use of the trade secrets.[150]

As with other aspects of monetary and equitable relief, the assessment of a damages award and its effect on the entitlement to injunctive relief is fact specific. In making such

---

of competitive damages would not be measurable in money damages)); *See also* Cutera, Inc. v. Lutronic Aesthetics, Inc., 444 F. Supp. 3d 1198, 1208 (E.D. Cal. 2020); TGG Mgmt. Co. v. Petraglia, No. 19-CV-2007-BAS-KSC, 2020 U.S. Dist. LEXIS 6376, at *22–23 (S.D. Cal. Jan. 14, 2020); Founder Starcoin, Inc. v. Launch Labs, Inc., No. 18-CV-972-JLS-(MDD), 2018 WL 3343790, at *13–14 (S.D. Cal. July 9, 2018).

148. *Sedona Trade Secret Equitable Remedies*, *supra* note 143, at 698 n.201 (collecting cases).

149. *Id*. at 720 n.245–46 (collecting cases).

150. *See, e.g.*, TMRJ Holdings, Inc. v. Inhance Techs., LLC, 540 S.W.3d 202, 209 (Tex. App. 2018) (finding that permanent injunction was not duplicative of lump-sum reasonable royalty award, stating: "[A] damages award that compensates a plaintiff for past damages combined with relief to prevent future damages does not constitute a double recovery."); Steves & Sons, Inc. v. Jeld-Wen, Inc., No. 3:16-CV-545, 2018 WL 6272893, at *4–5 (Nov. 30, 2018, E.D. Va.) (collecting cases for the proposition that reasonable royalties for past use of the trade secrets and permanent injunctions preventing future use can coexist without running afoul of the one-satisfaction rule).

determinations, courts often cite the positions the parties have taken throughout the case. For example, where the plaintiff's damages expert testified at trial about damages for harmful competition occurring in the future—and the jury instructions did not limit the temporal scope of damages (i.e., the concept of future damages was consistent with those instructions)—the damages award may be sufficient to make the plaintiff whole without need for injunctive relief.[151] Alternatively, damages awards for the development costs avoided by the misappropriating party may not be sufficient, absent an injunction, to compensate the plaintiff for harm from future unauthorized disclosures of

151. *Bladeroom Grp*., 2019 WL 1117537, at *3 (rejecting plaintiff's argument that permanent injunction was necessary to prevent harmful competition continuing into the future, citing testimony of plaintiff's damages expert purporting to quantify this injury: "Given this testimony, it is apparent BladeRoom believed at trial that its losses from future competition could be compensated with monetary damages . . . . Simply put, the trial evidence shows that BladeRoom's injury from future competition could be reduced to an amount of money, and a permanent injunction cannot be ordered merely because the requesting party did not receive the full extent of the legal relief it sought. The jury awarded BladeRoom the damages it found would fairly compensate BladeRoom for loss due to competition through 2020, and an injunction 'would be redundant of the legal relief which the jury has already awarded.'" (citations omitted)); Whiteside Biomechanics, Inc. v. Sofamor Danek Grp., Inc., 88 F. Supp. 2d 1009, 1020 (E.D. Mo. 2000) (denying permanent injunction, stating: "[T]he jury instructions did not limit the temporal scope of damages and that the concept of damages extending into the future is not inconsistent with the instructions given . . . . [P]laintiff's evidence and argument clearly contemplated and sought a damage award including future damages . . . . On this record, the Court concludes that the jury's damage award, though much smaller than plaintiff desired, represents the amount the jury believed would 'fairly compensate plaintiff for damages proximately caused by defendant's use of plaintiff's trade secrets' both to the date of verdict and in the future." (citation omitted)).

the trade secrets,[152] or for future gains from misappropriated trade secrets that had not been used or commercially implemented at the time of trial.[153]

Whether a permanent injunction may be duplicative of a lump-sum reasonable royalty award presents some unique issues. Generally, the jury (or court sitting in equity) calculates the amount of a lump-sum royalty based on a hypothetical negotiation of what a willing plaintiff and willing defendant would have settled on as a one-time payment to license the trade secrets at the time the misappropriation began. This negotiation often considers the future use of the trade secrets and the effect of that use on the parties' competitive positions.[154] In other words, a lump-sum reasonable royalty is often future-facing and may overlap with an injunction prohibiting the trade secrets' use. Some courts have refused to enter a permanent injunction in

---

152. Syntel Sterling Best Shores Mauritius Ltd. v. The TriZetto Grp., Inc., No. 15-Civ.-211-(LGS), 2021 WL 1553926, at *13 (S.D.N.Y. Apr. 20, 2021) (the award of damages for avoided development costs deemed inadequate compensation in view of trial record demonstrating likely dissemination of trade secrets in the future and resulting irreparable harm if this conduct was not enjoined; *rev'd and remanded*, 2023 WL 3636674, at *17 (2d Cir. May 25, 2023) in part in light of trial court's entry of permanent injunction barring further use or disclosure of trade secrets).

153. Syntron Bioresearch, Inc. v. Fan, No. D033894, 2002 WL 660446, at *12–13 (Cal. Ct. App. Apr. 23, 2002) (rejecting the argument that the entry of a permanent injunction enjoining future use or implementation of trade secrets that had not been used or commercially implemented as of the time of trial amounted to a double recovery — the damages award was distinguished as compensating plaintiff's actual losses and defendant's avoided development costs).

154. *TMRJ Holdings*, 540 S.W.3d at 210. ("The concept, in application, asks what a tortfeasor would have paid had it bought the technology rather than misappropriated it. The jury charge's definitions thus incorporate both the future earnings of the tortfeasor and the loss of revenue and future worth to the owner in determining the present value of the technology.").

addition to a lump-sum royalty on these grounds.[155] Others have found that permanent injunctive relief can coexist with a lump-sum royalty without running afoul of the double-recovery rule.[156] Equitable relief includes not just injunctive relief but also certain types of monetary remedies that are awarded by the court and not by the jury or fact-finder.[157] For example, both the

---

155. *See, e.g.*, *Steves & Sons*, 2018 WL 6272893, at *6–7 (denying permanent injunction in addition to lump-sum reasonable royalty, stating: "Having secured a reasonable royalty award based on what [the expert] told the jury, Jeld-Wen cannot now be heard to argue that Steves should be enjoined permanently from using the misappropriated trade secrets that [the expert] said that Steves could use for as long as it wanted in any way that it wanted if the jury would award damages in the amount of $9.9 million"). Cardiaq Valve Techs. v. Neovasc Inc., No. 14-cv-12405-ADB, 2016 WL 6465411, at *8 (D. Mass. Oct. 31, 2016) (denying permanent injunction in addition to a "future-facing" lump-sum reasonable royalty award that did not distinguish between past and future use of the trade secrets but rather approximated the sum that the defendant, in the fictional negotiation, would have been willing to pay to use the trade secrets indefinitely), *aff'd*, 708 Fed. App'x 654, 667–68 (Fed. Cir. Sept. 1, 2017).

156. *TMRJ Holdings*, 540 S.W.3d at 210–11 (While the court acknowledged that both the lump-sum royalty and the permanent injunction "conceivably redress [plaintiff's] future economic injury caused by [defendant]," it reasoned that the damages award alone did not make plaintiff whole for two reasons: first, the derivation of the royalty from the present value of the trade secrets to the defendant regardless of whether the plan to use them in the future comes to fruition; and second, the evidence showed that plaintiff never intended to make the trade secrets commercially available or to be licensed to third parties.); Sonoco Prods. Co. v. Johnson, 23 P.3d 1287, 1290 (Colo. App. 2001) (awarding lump-sum damages that plaintiff's counsel argued in closing represented both development costs and royalty for plaintiff's lost business; on this record there was no indication that damages were forward-looking or based on future gains realized by defendant related to the misappropriated information).

157. The focus of this *Commentary* is how to measure monetary remedies that may be available for trade secret misappropriation, including monetary "legal" remedies that are decided by the trier of fact as well as monetary

UTSA and the DTSA expressly provide that in exceptional circumstances an injunction may condition a defendant's future use on the defendant's payment of a reasonable royalty.[158] The comments to the UTSA describe this remedy as a "royalty order injunction" and indicate that exceptional circumstances are those rendering prohibitive injunctions inequitable or impractical, including "a person's reasonable reliance on acquisition of a misappropriated trade secret in good faith and without reason to know of its prior misappropriation."[159] The royalty order injunction should be distinguished from the separate statutory remedy allowing for the recovery of a reasonable royalty as an alternative form of compensatory damages.[160] The former is an equitable remedy awarded by the court; the latter is a legal remedy that, depending on the jurisdiction, is decided by either the court or the jury.[161]

Some courts have held certain other monetary remedies—including an accounting of profits, disgorgement of the misappropriator's profits, and the misappropriator's avoided research and development costs (at least those not offered as a proxy for the plaintiff's lost profits or royalties)—to be an equitable "restitution" for which there is no right to jury trial. Instead, the court

---

"equitable" remedies that are decided by the court sitting in equity. While *Sedona Trade Secret Equitable Remedies*, *supra* note 143, also discusses monetary equitable relief, it reserves for this *Commentary* the question of how to calculate this relief.

158. UTSA § 2(b); DTSA, 18 USC § 1836(b)(3)(A)(iii).

159. UTSA § 2(b), Cmt.

160. UTSA § 3(a), Cmt.

161. Steves & Sons, Inc. v. Jeld-Wen, Inc., No. 3:16-CV-545, 2018 WL 6272893, at *4 n.6 (the court distinguished between a royalty order injunction from the separate statutory remedy of reasonable royalty damages that had been awarded by the jury "under an entirely different provision, which allows for a reasonable royalty as a form of compensatory damages").

awards those remedies exercising its independent judgment.[162] In such cases, a jury may be asked for a nonbinding advisory opinion.[163]

6. Applying patent damages rules to trade secret damages analyses

Guideline No. 6 – Patent damages law and theory may or may not be applicable in a particular case, and care should be taken before importing patent damages law and theory.

It is sometimes suggested that patent damages law can be imported wholesale into trade secret cases. This is wrong. While it may be appropriate in certain instances to import certain aspects of patent damages law, noteworthy differences exist between litigation involving trade secret misappropriation and patent infringement, setting up unique challenges that should be evaluated before simply importing damages guidance from patent law.

To be sure, there is some overlap between the form of damages measures that may be awarded for patent infringement and those that may be awarded for trade secret misappropriation.[164]

---

162. *Sedona Trade Secret Equitable Remedies*, *supra* note 143, at 621 n.31 (collecting cases).

163. Order, Motorola Solutions, Inc. v. Hytera Commc'ns Corp., No. 1:17-CV-1973 (N.D. Ill. Oct. 19, 2020) D.I. 1088 (deemed jury award of avoided research and development costs under DTSA advisory); *id.*, Order (N.D. Ill. Jan. 8, 2021) D.I. 1099 (separate order awarding avoided research and development costs).

164. For a thorough discussion of patent damages, see the publications and presentations published by The Sedona Conference Working Group 9 (Patent Damages and Remedies) including, *e.g.*, The Sedona Conference, *Commentary on Patent Damages and Remedies, Public Comment Version* (June 2014) [hereinafter *Sedona Patent Damages*], *available at*: https://thesedonaconference.org/publication/Patent_Damages_and_Remedies, and The Sedona Conference,

While unjust enrichment may not be claimed in patent infringement (other than design patents), actual loss and reasonable royalties are available patent infringement remedies.

But it is also clear that trade secret misappropriation damages are unique and do not fit neatly into the patent infringement framework. Indeed, it is because of the many distinct differences between patent infringement and trade secret misappropriation that a more "flexible and imaginative"[165] approach propounded by the Fifth Circuit is necessary to properly compensate for the latter.

The following demonstrate some of the reasons for exercising caution in using patent damages law in trade secret cases:

- A plaintiff in patent infringement matters is always entitled to reasonable royalty damages at a minimum,[166] while royalty damages in trade secret litigation are not a floor and, depending on the jurisdiction, may not be available.
- There is a fundamental conceptual difference between a license for a trade secret and one for a patent: while patent infringement is a strict liability offense, trade secret misappropriation is not.
- A patent is a property right granted by a government that permits the owner to exclude others from practicing an invention for a defined period

---

Commentary on Patent Reasonable Royalty Determinations (Dec. 2016), *available at*: https://thesedonaconference.org/publication/Patent_Damages_and_Remedies.

165. Univ. Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 538 (5th Cir. 1974) (quoting Enter. Mfg. Co. v. Shakespeare Co., 141 F.2d 916, 920 (6th Cir. 1944)).

166. 35 U.S.C. § 284.

of time in exchange for public disclosure of the invention. A trade secret is information that derives independent economic value from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.

- To obtain a patent one must generally invent or discover a new and useful process, machine, manufacture, or composition of matter. A trade secret may comprise information that is not new or novel so long as the statutory elements of its definition are met.
- A patent infringer's actions cannot destroy the patent; even if a patent is infringed, a patent owner's right to exclude others from practicing the patent remains intact. A trade secret, however, may be destroyed when it is misappropriated and disclosed or used by the misappropriator.
- Patents have statutory terms. Trade secrets can have an indefinite life, which may—all else being equal—add value to them.
- Trade secrets can be used if they are discovered independently or reverse engineered. Patents cannot be used without a license until they expire.
- It is reasonable—indeed, common—for a patent owner and a licensee to make simultaneous use of a patent. That is not ordinarily true of a trade secret.

For these reasons, while the concept of a reasonable royalty for a license to use a patent makes evident economic and

business sense, that is not necessarily the case for a trade secret. Arguably, a hypothetical negotiation to license trade secrets to one's competitor is inconsistent with the inherent value of the trade secrets.

In addition, some courts have turned to apportionment principles from patent law when evaluating trade secret damages, such as consideration of the entire-market-value rule.[167] The entire-market-value rule dictates that "where multi-component products are involved, the governing rule is that the ultimate combination of royalty base and royalty rate must reflect the value attributable to the infringing features of the product, and no more."[168] Assuming the applicability of this rule to trade secret matters, plaintiffs can only recover damages for the value of the entire product where they can prove that the misappropriated features drive demand for the product as a whole, and, in fact, courts have excluded damages experts for failing to apportion damages to account only for the portion of the product that

167. For a background discussion of the entire-market-value rule, *see Sedona Patent Damages*, *supra* note 164, Section I.E.2 (Current State of the Law Regarding the Determination of a Reasonable Royalty—Entire Market Value Rule and Apportionment); for full discussion of the application of the entire-market-value rule for a patent reasonable royalty determination, *see id.*, Part III.B.1. (Determining the Royalty Rate—The Entire Market Value Rule (EMVR)).

168. MSC Software Corp. v. Altair Eng'g, Inc., No. 07-12807, 2015 WL 13273227, at *4 (E.D. Mich. Nov. 9, 2015) (citing VirnetX, Inc. v. Cisco Sys., Inc., 767 F.3d 1308, 1326 (Fed. Cir. 2014)) (excluding opinions of damages expert for failing to apportion damages to account for the portion of the product that came from the misappropriated trade secrets); *see also* Ford Motor Co. v. Versata Software, Inc., No. 15-CV-10628-MFL-EAS (consolidated with No. 15-11624), 2017 U.S. Dist. LEXIS 144833, (E.D. Mich Aug. 7, 2017) (citing to ResQNet.com, Inc. v. Lansa, Inc., 594 F.3d 860, 869 (Fed. Cir. 2010), a patent case, and excluding expert testimony which failed to apportion value between the features of the software protected by intellectual property and the other features).

came from the misappropriated trade secrets.[169] Of note, however, unlike in patent litigation where the patent at issue has limitations and claims, courts applying the entire-market-value rule in trade secret cases have allowed for "overall idea[s]" that contribute to the formation of a product, in addition to the misappropriated trade secrets, to be included in the royalty calculation.[170]

In short, courts, parties, and experts must consider the similarities and, importantly, the differences between patents and trade secrets when evaluating whether, and how, patent damages law may be applied in evaluating trade secret damages.

7. Improper acquisition but no use or disclosure

Depending on the jurisdiction, a plaintiff may or may not be entitled to recover damages for actual loss based on wrongful acquisition alone. For example, in *Oakwood Labs. v. Thanoo*, the Third Circuit examined the term "use" and found "[i]n accordance with its ordinary meaning and within the context of the DTSA, the 'use' of a trade secret encompasses all the ways one can take advantage of trade secret information to obtain an economic benefit, competitive advantage, or other commercial value, or to accomplish a similar exploitative purpose, such as

169. *Id*.

170. *See* Bianco v. Globus Med., Inc., No. 2:12-CV-00147-WCB, 2014 WL 5462388, at *18–19 (E.D. Tex. Oct. 27, 2014) (upholding a damages award based on the entire market value of a product where the defendant had previously paid royalties on the net sales of the entire product and the trade secrets related to the overall product, not a single subcomponent or feature); *see also* Steves and Sons, Inc. v. Jeld-Wen, Inc., No. 3:16-CV-545, 2018 WL 4844173, at *10 (E.D. Va. Oct. 4, 2018) (accepting damages expert's testimony that the reasonable royalty calculation did not, under the circumstances presented, need to be tied to a specific number of trade secrets but rather reflected a hypothetical payment for access to an entire field of knowledge, not knowing which intellectual property assets would be most important).

'assist[ing] or accelerat[ing] research or development.'"[171] The court also rejected the district court's view that because the plaintiff had not alleged that it had suffered lost sales or investment opportunities or partnerships because of the defendants' actions, it could not state a claim for misappropriation. "By statutory definition, trade secret misappropriation *is* harm . . . . [E]ven if it is true that the Defendants have not yet launched a competing product, that does not mean that Oakwood is uninjured. It has lost the exclusive use of trade secret information, which is a real and redressable harm."[172]

Similarly, a trade secret holder may be entitled to injunctive relief and attorneys' fees (where the misconduct is sufficiently egregious) based on threatened misappropriation or where there is actual misappropriation but no actual loss.

Plaintiffs have also attempted to secure nominal damages as distinct from actual damages for statutory-based trade secret misappropriation.[173] In certain instances, however, courts have held that there is no recovery of nominal damages for statutory-based trade secret misappropriation.[174]

---

171. 999 F.3d 892, 910 (3d Cir. 2021) (citation omitted).

172. *Id.* at 913–14 (citations omitted).

173. Nominal damages refers to damages inferred as a matter of law or policy upon the showing of the invasion of a legal right, as opposed to monetary relief awarded upon proof of actual injury, loss, or harm. *See* AlphaMed Pharms. Corp. v. Arriva Pharms., Inc., 432 F. Supp. 2d 1319, 1335–36 (S.D. Fla. 2006) (The court distinguished between recovery of nominal damages under Florida common law and damages available under Florida's UTSA: "To be sure, Florida law does permit the award of nominal damages 'when the breach of an agreement or invasion of a right is established, since the law infers some damage to the injured party, where there is insufficient evidence presented to ascertain the particular amount of loss, the award of nominal damages is proper.'" (citations omitted)).

174. This principle was apparent in *MSC.Software Corp. v. Altair Eng'g, Inc.*, 281 F. Supp. 3d 660, 661 (E.D. Mich. 2017), in which the court granted

defendant's motion for summary judgment after plaintiff's damages expert had been excluded in a Daubert order, holding that "the weight of authority holds that MSC is not entitled to nominal damages under the circumstances." *Id*. The authority considered by the court in *MSC* included a leading case out of the Eleventh Circuit, *AlphaMed Pharms.*, 432 F. Supp. 2d at 1335–36, *aff'd*, 294 Fed. App'x 501 (11th Cir. 2008) in which the court vacated a jury award of nominal damages of $1 for trade secret misappropriation under Florida's UTSA. The court expressly held that nominal damages are not recoverable under the UTSA and granted judgment as a matter of law in defendants' favor based on plaintiff's failure to satisfy its burden of proving actual damages. *Id*.

THE SEDONA CONFERENCE COMMENTARY ON THE GOVERNANCE AND MANAGEMENT OF TRADE SECRETS

A Project of The Sedona Conference Working Group 12 on Trade Secrets

Author:

The Sedona Conference

Editors-in-Chief:

James Pooley Victoria Cundiff

Managing Editors:

Jim W. Ko Casey Mangan

Senior Editors:

Nicole D. Galli
Elizabeth McBride
Jennifer Lynn Miller

Contributing Editors:

Cassius A. Elston
David Prange
Nicholas Steele

Staff Editor:

David Lumia

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference's Working Group 12. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any organizations to which they may

belong, nor do they necessarily represent official positions of The Sedona Conference.

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, 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 Governance and Management of Trade Secrets*, 24 SEDONA CONF. J. 429 (2023).

PREFACE

Welcome to the July 2023, Final, Post-Public Comment Version of *The Sedona Conference Commentary on the Governance and Management of Trade Secrets*, a project of The Sedona Conference Working Group 12 on Trade Secret Law (WG12). 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 WG12, formed in February 2018, is "to develop consensus and nonpartisan principles for managing trade secret litigation and well-vetted guidelines for consideration in protecting trade secrets, recognizing that every organization has and uses trade secrets, that trade secret disputes frequently intersect with other important public policies such as employee mobility and international trade, and that trade secret disputes are litigated in both state and federal courts." The Working Group consists of members representing all stakeholders in trade secret law and litigation.

The WG12 *Commentary* drafting team was launched in November 2018. Earlier drafts of this publication were a focus of dialogue at The Sedona Conference on Trade Secrets in Denver, Colorado, in May 2022, The Sedona Conference WG12 Annual Meeting 2021, in Phoenix, Arizona, in December, 2021, the WG12 Annual Meeting, Online, in November 2020, the WG12 Annual Meeting in Charlotte, North Carolina, in November 2019, and the WG12 Inaugural Meeting in Los Angeles, California, in November 2018. The editors have reviewed the comments received through the Working Group Series review and comment process.

This *Commentary* represents the collective efforts of many individual contributors. On behalf of The Sedona Conference, I thank in particular James Pooley, the Chair Emeritus of WG12, and Victoria Cundiff, the Chair of WG12, who serve as the Editors-in-Chief of this publication, and Nicole D. Galli, Elizabeth McBride, and Jennifer Lynn Miller, who serve as the Senior Editors of this publication. I also thank everyone else involved for their time and attention during this extensive drafting and editing process, including our Contributing Editors Cassius A. Elston and David Prange, and also Nicholas Steele.

The drafting process for this *Commentary* has also been supported by the Working Group 12 Steering Committee and Judicial Advisors. The statements in this *Commentary* are solely those of the nonjudicial members of the Working Group; they do not represent any judicial endorsement of any recommended practices.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG12 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, data security and privacy liability, patent remedies and damages, and patent litigation best practices. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be.

Craig W. Weinlein
Executive Director
The Sedona Conference
July 2023

TABLE OF CONTENTS

FOREWORD

This *Commentary* was written from both legal and business perspectives as a useful reference for the design and implementation of trade secret governance and protection programs in corporate environments. It can also provide insight to litigators and judges about the practical ways companies approach the "reasonable efforts" requirement in trade secret law. The central message is that programs to manage trade secrets, like other business processes, should align with business objectives *in the context of the needs of the specific business*. Ideally, trade secret management should be contextual and strategic, and not just a collection of "boilerplate" forms and protocols that may bear little relationship to the actual trade secrets and risk environment of a particular company.

While trade secret management demands strategic business thinking, it also has a legal dimension. The existence of a trade secret depends in part on whether the company has exercised "reasonable efforts" (or "reasonable measures") directed at maintaining its secrecy. This standard corresponds to the relevant circumstances of each enterprise, so that there can be no "one size fits all." In effect, it suggests that the judge or jury apply the same kind of analysis; namely, an assessment of the value of, and risks to, specific trade secrets in the context of the company's particular business and resources. We hope that this paper will help management formulate a proactive, tailored, and practical approach to managing trade secret assets that will address both business and legal requirements.

This *Commentary* differs from some other Sedona Commentaries not only in its intended audience but also in its focus on "issues to consider" rather than on developing specific guidelines that may be seen as insufficiently flexible. By thinking through the questions raised by this *Commentary* and utilizing the framework for the design and implementation of trade

secret management programs provided, companies will more effectively exercise control over their trade secrets and understand the value of sustained investment to that end.

James Pooley
Victoria Cundiff
Editors-in-Chief and Working Group 12
Steering Committee Chair Emeritus and Chair

Nicole D. Galli
Elizabeth McBride
Jennifer Lynn Miller
Senior Editors

GOVERNANCE AND MANAGEMENT OF TRADE SECRETS PRINCIPLES AT A GLANCE

PRINCIPLE No. 1 – Trade secrets should be protected by efforts that are reasonable under the circumstances to maintain their secrecy and value. Absolute secrecy is neither possible nor required. There is no one-size-fits-all approach.

PRINCIPLE No. 2 – A trade secret protection program should be actionable and achievable, rather than conceptual or aspirational. Once implemented, it should be periodically evaluated and adjusted as the company's trade secrets, business, and risk environment evolve.

PRINCIPLE No. 3 – A trade secret protection program should align with business goals and measurable objectives such as (1) securing and maintaining competitive advantage for the business; (2) leveraging trade secrets to commercialize new products and services; (3) supporting, generating, and incentivizing continued innovation; (4) extracting additional value from trade secrets through licensing, acquisitions, or secured financing; and (5) enforcing trade secret rights as necessary.

PRINCIPLE No. 4 – Trade secret governance generally requires an integrated enterprise approach that should accommodate and satisfy multiple and potentially conflicting corporate interests, including effective controls, information governance and data security, talent acquisition and retention, operational efficiency, disciplined budgets, reasonable return on investment, third-party information sharing demands, and legal enforceability.

I. INTRODUCTION

Trade secrets are intellectual property assets whose value stems from secrecy and the competitive advantage provided to their owner. Because trade secrets can also be cultivated, maximized, and profitably exploited along with other corporate assets, they can contribute to increasing the overall value of the business. Financial markets increasingly look to leverage trade secrets as assets in a range of transactions, including, in many cases, in mergers and acquisitions, licensing, securing loans, and risk transfer solutions.

But not all trade secrets are alike, nor are the businesses that seek to exploit them. Business success and progress often derive from not just one but many categories of confidential information. The Coca-Cola Company does not rely solely on the formula for its famous beverage. Like other businesses, it also has secrets related to product road maps; product modifications for multiple markets; planned advertising campaigns; sources of key ingredients; and research and development programs. Some of this information needs to be shared in a controlled fashion with people within and outside the organization, while other trade secrets may best be protected by keeping them locked away for occasional reference by a select few.

The value of particular trade secrets, the risks they face, and the effectiveness of controls may all change over time, particularly as the trade secret owner and its business operations and goals evolve. Some information will lose protection when a product is released or a patent issues, while other trade secrets may remain valuable indefinitely. Future technologies or market conditions may render a secret obsolete; or the success of a product or division may grow, and along with it the value of the related secrets. Resource constraints or operations flows affecting a company's ability to adopt certain security measures may vary over the life cycle of the trade secret. So too, the risks to

trade secrets are often dynamic, affected by changes in the workforce or in supply chains. And they may be amplified by externalities such as cybertheft or the shift to more remote work.

For all these reasons, protecting trade secrets is almost never a "once and done" project—it is a process to be evaluated over time as the nature and value of trade secrets to a company shift and as the company itself evolves. Further, protecting trade secrets cannot happen in isolation: trade secrets may be part of a larger portfolio of intellectual property assets that needs to be managed in accordance with the rules for each applicable legal regime. While every invention conceivably can be protected for at least some period of time as a trade secret, the long-term protectability of particular information as a trade secret may evolve as patents and copyrights are sought and issued.

Trade secret programs should be designed, in the first instance, under the scrutiny of business leaders and other relevant stakeholders. This allows decisions on investment in security to align with perceived value of the information and the operations and overall goals of the company and the interests of its various business units or functions.[1] In this way, trade secret protection programs will be integrated with strategic

1. Because we are speaking to business leaders who evaluate the need for and effectiveness of trade secret programs primarily in business terms, this *Commentary* employs some business terminology. For example, "return on investment (ROI)" refers to recapturing in the future what is invested today, together with an additional amount representing the risk to capital. A trade secret owner may realize a return on its investment not only by using information to increase internal efficiency and by better leveraging advantages commercially, but also or alternatively through licensing the information to third parties or avoiding costly litigation. Another example is "key performance indicators" ("KPI"), a set of metrics used to track performance of a person, business unit, product, or goal. The KPI metrics for a particular program are set up in advance to track performance, often through a "dashboard" or other reporting tool.

management. Of course, such programs must also be informed by legal considerations.

The law requires that trade secrets be protected with "reasonable measures" to maintain secrecy.[2] What is "reasonable" implies an inherently fact-specific analysis, so the case law can provide only general guidelines for companies to consider.[3] In general, when establishing policies, controls, and other mitigation measures, the owner should consider the value of the information assets, the risks of loss or contamination, the effectiveness and cost of potential policies, controls, and other measures, as well as the practical realities of the business's operations and strategic goals.

Because the legal framework is contextual, there can be no definitive set of "best practices" in developing a trade secret protection program. Rather, each company should choose an approach that fits its unique business circumstances as well as its most valuable information. While perfection is not required, thoughtful care and attention to the needs of the specific organizational context are.[4] This *Commentary* seeks to provide

---

2. 18 U.S.C. § 1839(3)(A); *see also* Uniform Trade Secrets Act § 1(4)(ii) (requiring "efforts that are reasonable under the circumstances").

3. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. c (Am. Law Inst. 1995).

4. Several research studies have found that most companies rely on fairly rudimentary measures to protect their trade secrets, e.g., confidentiality and noncompete agreements, general cybersecurity protection, employee policies, and enforcement efforts. *See, e.g.*, BAKER MCKENZIE, THE BOARD ULTIMATUM: PROTECT AND PRESERVE, THE RISING IMPORTANCE OF SAFEGUARDING TRADE SECRETS (2017), https://www.bakermckenzie.com/-/media/files/insight/publications/2017/trade-secrets; David S. Almeling, et al., *A Survey of In-House Attorney Views on Trade Secrets*, LAW360 (Jan. 12, 2018), https://www.law360.com/articles/999664/a-survey-of-in-house-attorney-views-on-trade-secrets. Some courts may reject such measures as "normal business practices" insufficient to meet the "reasonable measures"

companies with an outline of issues to be evaluated, an array of sample measures that can be considered for implementation, and an overall framework for assessing the relevant circumstances and designing and implementing a program sufficient to meet the company's ongoing needs.[5]

Principle No. 1 – Trade secrets should be protected by efforts that are reasonable under the circumstances to maintain their secrecy and value. Absolute secrecy is neither possible nor required. There is no one-size-fits-all approach.

Whether viewed through the legal lens of "reasonable" measures, or as a process of classical corporate asset management comparing risks, value, and rewards, the imperatives are the same. To protect the integrity of what it owns and preserve its ability to enhance enterprise value, the company should define in some practical way its most important secrets, so that it

---

standard. *See, e.g.*, Opus Fund Servs. (USA) LLC v. Theorem Fund Servs., LLC, No. 17 C 923, 2018 WL 1156246, at *3 (N.D. Ill. Mar. 5, 2018) (dismissing complaint).

5. Other related Sedona Conference commentaries provide useful guidance as well, including: The Sedona Conference, *Commentary on Privacy and Information Security*, 17 SEDONA CONF. J. 1 (2016), https://thesedonaconference.org/publication/Commentary_on_Privacy_and_Information_Security; The Sedona Conference, *Commentary on Information Governance, Second Edition*, 20 SEDONA CONF. J. 95 (2019), https://thesedonaconference.org/publication/Commentary_on_Information_Governance; 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), https://thesedonaconference.org/publication/Commentary_on_Application_of_Attorney-Client_Privilege_and_Work-Product_Protection_to_Documents_and_Communications_Generated_in_the_Cybersecurity_Context; The Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 SEDONA CONF. J. 495 (2018), https://thesedonaconference.org/publication/Commentary_on_BYOD.

can assess their value relative to the cost (in money or administrative inconvenience) of maintaining control through various security measures and to educate its workforce on what needs protection. While various checklists or examples of security measures (such as those in Appendix A) may be helpful references, only the company's management can be aware of the cost-benefit variables, corporate culture, existing operations and systems, and business goals that will drive decisions regarding protection of its own information. This *Commentary* is intended to provide a review of the legal and business landscape related to trade secret protection, including the array of factors that should be considered by all sizes and kinds of companies when developing the company's approach to trade secret protection, whether the company be a "mom and pop" business or a large global enterprise.

Principle No. 2 – A trade secret protection program should be actionable and achievable, rather than conceptual or aspirational. Once implemented, it should be periodically evaluated and adjusted as the company's trade secrets, business, and risk environment evolve.

No program or policy is effective if it is only published in a document. Aspirational standards that are never implemented or consistently followed are at best counterproductive. Among other things, defense counsel in litigation may seek to exploit the trade secret owner's failure to adhere to stated policies and procedures as a reason to block enforcement. An important element of building a sustainable trade secret governance approach consists of effective implementation and compliance, measured by appropriate controls across the company and its workforce. A court may ultimately find that the legal standard was met if key portions were implemented and consistently followed, even without complete fidelity to the program charter or

policy. But lapses can present otherwise avoidable challenges during litigation.

II. INHERENT CHALLENGES TO DEVELOPING A TRADE SECRET PROTECTION PROGRAM

A. The Legal Framework for Protecting Trade Secrets Provides Limited Concrete Guidance in the Face of Complex Organizational Factors

The range of information eligible to be a trade secret is vastly broader than patent- and copyright-eligible subject matter and can include virtually any information that provides a competitive advantage. State and federal laws and reported decisions have found a wide variety of information eligible to be a trade secret. Frequent candidates for protection as a trade secret include business plans, marketing roadmaps, organizational designs, algorithms, proprietary data sources and databases, technical drawings, source code, recipes, formulas, new product specifications, manufacturing processes, and concrete business strategies.

The fact that information may be eligible to be a trade secret, however, does not mean that in a particular case it will ultimately be found to be a trade secret. The Uniform Trade Secret Act (UTSA), state implementations of the UTSA, and the federal Defend Trade Secrets Act (DTSA) all include as part of the definition of a trade secret the requirement that the information must be the subject of "reasonable measures" to protect it.[6] Decisions in some jurisdictions under both the UTSA and the DTSA are also still influenced by the Restatement (First) of Torts, referencing the "extent of measures taken to protect the

6. *See* 18 U.S.C. § 1839(3)(A) (2016); *e.g.*, CAL. CIV. CODE § 3426.1(4) (2006); 765 ILL. COMP. STAT. 1065/2(d)(2) (1988); MINN. STAT. § 325C.01 Subd. 5(ii) (1986); Uniform Trade Secrets Act § 1(4)(ii) (1985).

information" as one of a set of factors to be considered in determining whether there is a trade secret.[7]

The legal framework for protecting trade secrets in the United States can vary from state to state. Federal law echoes the theme that trade secrets must be subject to reasonable measures to protect them and must not be readily ascertainable by others who can obtain value from them, but it generally does not impose specific requirements as to what the protection measures must be. The laws of other countries will be pertinent for companies that operate internationally; some of these laws spell out precise requirements that must be followed to protect trade secrets within that jurisdiction. Other commentaries have provided extensive analysis of key statutory regimes, and we rely on those to inform our analysis here.[8]

Reported judicial decisions throughout the United States, while finding certain behavior to suffice or fall short of "reasonable," focus primarily on unique facts of the case.[9] Therefore,

---

7. *See* Ashland Mgmt. v. Janien, 624 N.E.2d 1007, 1013 (N.Y. 1993) (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW INST. 1939)); *see also* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. L. INST. 1939). *But see* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (AM. L. INST. 1995) (not including within definition of "trade secret" a requirement that information be protected by measures that are reasonable under the circumstances).

8. For survey of trade secret laws in key U.S. states, *see generally* The Sedona Conference, *Commentary on Protecting Trade Secrets Throughout the Employment Life Cycle*, 23 SEDONA CONF. J. 807 (2022), https://thesedonaconference.org/publication/Commentary_on_Protecting_Trade_Secrets_Throughout_Employment_Life_Cycle [hereinafter *Sedona Employment Life Cycle Commentary*]. For survey of trade secret laws in key non-U.S. countries, *see generally*, The Sedona Conference, *Framework for Analysis on Trade Secret Issues Across International Borders: Extraterritorial Reach,* 23 SEDONA CONF. J. 909 (2022), https://thesedonaconference.org/publication/Trade_Secret_Issues_Across_International_Borders_Extraterritorial_Reach.

9. *See, e.g.*, Tax Track Sys. Corp. v. New Inv. World, Inc., 478 F.3d 783, 787 (7th Cir. 2007) ("The question here is how much effort to keep

while case law can be informative, it offers little in the way of concrete guidance from which a company can design and implement its own strategy to protect trade secret assets.[10]

Along with these intentionally elastic legal assessments made in the context of specific cases that often do not give detailed insight into the business organization involved, companies must contend with different business and development environments, along with, in many cases, competing internal corporate programs and priorities and preexisting information

---

information confidential is enough to be considered reasonable? Courts evaluate this question on a case-by-case basis, considering the efforts taken and the costs, benefits, and practicalities of the circumstances . . . . Typically, what measures are reasonable in a given case is an issue for a jury . . . . In some circumstances, however, it may be readily apparent that reasonable measures simply were not taken.") (internal citations omitted); Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179 (7th Cir. 1991) ("[O]nly in an extreme case can what is a 'reasonable' precaution be determined on a motion for summary judgment, because the answer depends on a balancing of costs and benefits that will vary from case to case and so require estimation and measurement by persons knowledgeable in the particular field of endeavor involved."); Mattel, Inc. v. MGA Ent., Inc., 782 F. Supp. 2d 911, 959 (C.D. Cal. 2010) ("The determination of whether information is the subject of efforts that are reasonable under the circumstances to maintain its secrecy is fact specific."); Data Gen. Corp. v. Grumman Sys. Support Corp., 825 F. Supp. 340, 359 (D. Mass. 1993) ("Whether reasonable steps have been taken depends on the circumstances of each case, including the nature of the information sought to be protected and the conduct of the parties.").

10. *But see* NEV. REV. STAT. § 600A.032 (2001), the Nevada Trade Secret Statute, establishing that "[t]he owner of a trade secret is presumed to make a reasonable effort to maintain its secrecy if the word 'Confidential' or 'Private' or another indication of secrecy is placed in a reasonably noticeable manner on any medium or container that describes or includes any portion of the trade secret. This presumption may be rebutted only by clear and convincing evidence that the owner did not take reasonable efforts to maintain the secrecy of the trade secret." Some foreign trade secret laws also impose more formalistic requirements than the contextual "reasonable efforts" standard.

technology systems. Potentially conflicting company strategies and objectives must be considered, as well as the practical realities of running a business. Company priorities and resources may shift over time. These variables can make it difficult to build support and secure budgets. These challenges can be frustrating to business leaders focused on execution (and those tasked with protecting intellectual property) and can lead to inconsistent and ineffective implementation and compliance.

Many different inputs can affect a decision about what measures are reasonable within a particular organization. Companies come in all shapes and sizes and industries, and they manage different risks and challenges in designing, implementing, and sustaining such measures, while also absorbing the related cost and operational burdens. While most companies need to make some disclosures of their trade secrets to capture value from them, companies differ in the extent to which they need, or strategically choose, to disclose information both internally and externally. Companies may be required or elect to disclose some trade secrets to suppliers, to government agencies, or across borders, presenting additional risks and challenges. Research-focused organizations may choose to extend access to a broad group of personnel and also to outside contractors or collaboration partners, both private and public. Companies in some fields may face market or business pressures to seek patent protection for some innovations, which may impact the issue of what related information can later be claimed as a trade secret.[11] On top of these sometimes conflicting demands, the

11. *See, e.g.*, Hickory Specialties, Inc. v. Forrest Flavors Int'l, Inc., 12 F. Supp. 2d 760 (M.D. Tenn. 1998), *aff'd* 215 F.2d 1326 (6th Cir. 2000) (holding that information disclosed in a patent is not protectable as a trade secret even if the patent was not the source of defendant's access to the information at issue). However, the issue of whether a patent negates a trade secret is nuanced as courts have also recognized that a patent has not resulted in lost

business may have to contend with different policies and systems as well as the objectives and practices of key functions such as information technology (IT), human resources (HR), security, legal (potentially including patent as well as other legal teams), communications, and marketing.

The nature of the secret information can also significantly impact whether reasonable measures have been employed to protect it. Trade secrets can be expressed, stored, and secured in many different ways and embodiments. Some information can be productively shared through providing highly restricted access to only a handful of people, while other information may need to be shared more broadly to multiple constituencies to effectively operate key business functions. Some trade secrets, such as prototype equipment on a manufacturing floor, require physical security measures. And a large amount of trade secret information is stored and communicated digitally, potentially necessitating use of sophisticated technological as well as

---

trade secret protection. *See also* Allied Erecting and Dismantling Co., Inc., v. Genesis Equip. & Mfg., Inc., 649 F. Supp. 2d 702 (N.D. Ohio 2009)("while, as a general proposition, there is no trade secret protection for secrets that are disclosed in a patent application, numerous courts have allowed trade secret protection for processes or specifications related to the patented device that are not disclosed in the patent."); Tex. Advanced Optolectronic Sols., Inc. v. Renesas Elecs. Am., Inc., 895 F.3d 1304 (Fed. Cir. 2018) (patent must disclose combination of elements that comprises trade secret to render trade secret protection extinguished); Wellogix, Inc. v. Accenture, L.L.P., 716 F.3d 867 (5th Cir. 2013) ("patent destroys the secrecy necessary to maintain a trade secret only when the patent and trade secret both cover the same subject matter."); AgroFresh Inc. v. Essentiv LLC, C.A. No. 16-662 (MN), 2020 WL 7024867, at *5 (D. Del. Nov. 30, 2020) (trade secret protection not lost through publication because it did not reveal specific mechanisms protected by trade secret); Celeritas Techs. Ltd. v. Rockwell Int'l Corp., 150 F.3d 1354 (Fed. Cir. 1998) (upholding verdict that information in the patent was not readily ascertainable because the "implementation and techniques" protected by trade secret "went beyond the information disclosed in the patent").

contractual controls, sometimes including controls such as multifactor authentication, biometric identification, or otherwise highly restrictive access management.

Companies often look to benchmarking data, where available, in order to design new programs and policies, hoping to become better informed and borrow from "best practices" and industry leaders. Such an approach may indeed be helpful to inform the process but should not be relied on as the sole basis for design; the variation in circumstances among businesses means that "borrowing" of generalized strategies can result in expensive overkill or leave major gaps in a protection plan.

B. Generic Confidentiality Measures Can Be Effective but Carry Their Own Risks

Various checklists, frequently promoted by security vendors or in alerts proposing security audits, suggest that adequate protection can be provided by certain general practices, such as employee and third-party confidentiality agreements, facilities security, and robust IT systems. These generic practices or general confidentiality approaches can be helpful as a starting point and in some cases can be adequate protection. But relying only on generalized checklists and generic approaches, without critical analysis as to their adequacy or applicability to the needs of the particular information and company, can instill a false sense of security for the simple reason that most businesses face a unique set of risks regarding a unique set of valuable information assets. Generic programs tend to homogenize the risk across business in general or a given industry. Generalized approaches can only address the risks mitigated by these baseline measures, and not any risks that are peculiar to a company's own information, operations, and business. For example, consider "customer information," which can be extremely valuable in the abstract. Very little in the way of specific security measures may be necessary for a small business where a

customer list is known to and accessible by only the two owners, while much more may be required to protect a broader scope of customer information at a large company with a sales force, accounting staff, and customer service representatives who work closely with assigned accounts, and where sophisticated analytic tools are used to model, predict, and influence customer behavior or to assess competitive offerings. Further, "standard" measures may become "shop worn" and may not reflect evolving case law or new contractual or technological tools for companies to consider.

C. *Attorney-Client Privilege and Business Records: A Double-Edged Sword*

Designing and administering trade secret programs present special challenges around protecting attorney-client privilege during company operations and processes. Ideally, counsel (whether in-house or external) should assist in the identification of trade secrets and formulation of a trade secret protection effort. There are many nuanced legal issues involved with identifying what is a trade secret, how the program will be evaluated as "reasonable" in an enforcement action, optimal contract protections, and the like. It may also be helpful to have attorney-client privilege attach to the communications among those doing this work without worry that it will later be subject to discovery and attack by opposing counsel in an enforcement action. The same is true for compliance efforts, periodic reviews of the program, and investigations related to potential losses and enforcement. This protection from disclosure to promote candor is why the attorney-client privilege exists—so that these valuable legal communications are not stifled.

However, in a later enforcement action, a company may want to present internal communications that identify the relevant trade secrets or document its protection efforts. If such efforts are solely reflected in communications with the legal

department, production of the communications in litigation may risk a broad subject-matter privilege waiver. Therefore, it is equally important when designing a protection program to consider what information and documentation the company would like to treat as a "business record" that can be used without waiving any attorney-client privilege. For example, once trade secrets have been identified with legal input, some companies choose to create a business record to identify the trade secrets as part of a training and compliance program aimed at protecting them. This nonprivileged record can be used to make sure the appropriate staff know what the trade secrets are and what security measures are required to protect them. Where appropriate, such records can also become part of a document retention policy or exit interview protocol. These business records can be put forward in any enforcement action without jeopardizing privileged communications.

If counsel providing advice to the team is in-house, the privilege issues can be more complicated. This is particularly true in smaller companies where in-house counsel can have several roles, some of which are more business related than legal. In this situation, some communications with these persons are privileged (where they are providing legal advice) and some are not (where they are performing, for example, an HR or purely business strategy function). Under these circumstances, it is particularly important to understand and act purposefully in making judgments before any litigation about what information is and is not intended to be privileged and to mark documents and consider information flows accordingly.

III. DEVELOPMENT OF THE TRADE SECRET PROTECTION PROGRAM

Implementation of a trade secret protection program generally consists of three steps. The first step is designing the program, including identifying the information to be protected and evaluating and choosing appropriate protective measures. The second consists of implementing the program in a way that breathes life into the chosen policies, processes, and controls. Third is building and sustaining compliance, which includes periodic assessment and updates of the program to ensure it continues to provide adequate protection in the face of changes to the external environment and to the company's trade secrets, risk environment, operations, and strategic goals.

Principle No. 3 – A trade secret protection program should align with business goals and measurable objectives such as (1) securing and maintaining competitive advantage for the business; (2) leveraging trade secrets to commercialize new products and services; (3) supporting, generating, and incentivizing continued innovation; (4) extracting additional value from trade secrets through licensing, acquisitions, or secured financing; and (5) enforcing trade secret rights as necessary.

While designing and implementing a protection program can require extensive executive engagement, sustained investment, and enterprise discipline, the reality is that there are usually existing processes and practices that can be leveraged for this purpose. In some cases, the bulk of the effort lies in simply centralizing (and sometimes harmonizing) these other processes for the governance of trade secrets in a manner that will meet a "reasonable efforts" standard.

The success of a program often depends on executive leadership and business general managers "buying in" to the value

of the secrets and the measures needed to protect them. This support may be necessary to justify the cost, as well as to establish the "tone at the top" that is so important in driving compliance. For these reasons, it is important to identify all stakeholders at the beginning of the project, and to think about the company's goals and the range of benefits and return on the investment (ROI) that the program can deliver.

<u>Principle No. 4</u> – Trade secret governance generally requires an integrated enterprise approach that should accommodate and satisfy multiple and potentially conflicting corporate interests, including effective controls, information governance and data security, talent acquisition and retention, operational efficiency, disciplined budgets, reasonable return on investment, third-party information sharing demands, and legal enforceability.

A. Preliminary Steps

1. Articulate the value of the program and its return on investment

Within the last quarter century, intangible property has emerged as the single most significant asset of S&P 500 companies. A 2020 study by Ocean Tomo concluded that the share of intangible asset market value (primarily intellectual property) of the S&P 500 increased from 68 to 84 percent between 1993 and 2015, and COVID-19 accelerated that trend, with intangible assets now commanding over 90 percent of the S&P500 market value.[12] A trade secret protection program, when understood in

12. A summary of the current Ocean Tomo study is available at *Ocean Tomo Releases Intangible Asset Market Value Study Interim Results for 2020*, OCEAN TOMO (Sept. 22, 2020), https://www.oceantomo.com/media-center-

the context of protecting a company's core value, is increasingly important to the company. Framing the effort in a way that emphasizes the return on investment (ROI) is important to gain buy-in from stakeholders and the sustained investment required. The "return" can be in the form of asset values identified, created, increased, or extracted. It can also be expressed in the form of the support the program provides the company in achieving its goals and improving financial performance, as well as in the company avoiding costs associated with loss of its trade secrets or liability for mishandling the secrets of others.

Substantiating an ROI can be achieved in numerous ways. The most rudimentary example is for the owner to calculate the value of the secrets to be protected and compare the cost of the protection against the value of preserving and building that value. By statutory definition, trade secrets must have "actual or potential economic value." Companies can extract commercial value for their trade secrets by using them internally to achieve a market advantage over competitors who do not know them. Companies have been able to achieve a market advantage from their trade secrets through innovating new products, through realizing and maintaining higher margins for their products, or through being "first to market" and continuing to preserve a "lead time" advantage even after others enter the field. Many companies have been able to obtain commercial value from their trade secrets through a variety of commercial transactions as well. Some companies, for example, in the semiconductor, petrochemical, and biopharmaceutical industries, have additionally extended their economic reach and achieved substantial value through licensing activity, either by licensing transactions with customers who are willing to pay to gain access to trade secrets they can exploit for themselves, or by

---

item/ocean-tomo-releases-intangible-asset-market-value-study-interim-results-for-2020/.

licensing trade secrets to third parties who may have greater access to particular markets than the trade secret owner does. More recently, a growing number of companies have also been able to derive value for their trade secrets in capital-raising and merger-and-acquisition transactions, by increasing their overall valuation in determining the equity offering or purchase price. A successful protection program will help substantiate, maintain, and even boost this value of core trade secret assets, such as by enabling the use of trade secrets as collateral for financing or for transferring risk with insurance solutions.

Another effective way to show a return on investment may be to determine what costs will be avoided by risk mitigation and properly protecting the trade secret assets. For instance, for a company concerned about misappropriation risk, the prevention of a single incident can avoid significant cost, since even a relatively small dispute can often run into millions of dollars in litigation costs alone,[13] as well as disruption to business processes and distraction to company personnel. And there also can be avoidance of other less direct costs, for example from lost sales, new product delays, lost market share, and reputational damage. A thorough financial estimation of the cost avoidance and risk mitigation that an effective program delivers will serve as a useful foundation for determining ROI.

Another helpful approach is to consider the enterprise value creation of a comprehensive program. This can be calculated based on multiple factors, such as the estimated direct value and improved financial performance that core competitive advantages deliver to the business (e.g., higher margin sales).

13. AIPLA, REPORT OF THE ECONOMIC SURVEY I-225 (2021) (mean cost to litigate a trade secret misappropriation case involving risk of greater than $25 million, inclusive of discovery, pretrial, trial, posttrial, and appeal, at $4.582 million, and first and fourth quartile of respondents reporting litigation costs of $1.5 million and $8 million, respectively).

Indeed, an effective trade secret protection program not only focuses on providing robust protection and supporting a strong enforcement position but can also serve as a catalyst for inspiring and reinforcing a culture of innovation—and the creation of new trade secrets. In this respect, an ROI can be derived based on the value attributable to these new innovations and how they explicitly map to value chains and select product lines. The ROI calculation can also consider the value of prevention of loss of institutional knowledge, because the program can ensure the consistent documentation of that knowledge.

In considering the investment side of the equation, it is important to consider the company's ability to leverage any existing systems or processes to protect the secrets, thereby avoiding the expense and operational distraction of developing these systems from scratch.[14]

2. Identify all potential stakeholders

For many companies, the information, input, and buy-in will come from different functional areas of the company, such as legal, human resources, information technology, data owners, executive leadership, finance, risk management, supply chain and vendor management, communications, regulatory, research and development, business development, and various operating divisions or business units. Even within these groups, there may be differing perspectives or priorities to take into consideration (e.g., intellectual property, commercial, and corporate governance counsel may have very different points of view on some program measures).[15] Many companies form a cross-

14. *See infra* Section III.B.4 (Integrated enterprise approach: Leverage existing capabilities and processes and navigating conflicting or competing objectives).

15. Companies in some fields may face market or business pressures to seek patent protection for some innovations, which would benefit from close

functional team, including representatives from each of these functions (or a smaller team may tap into these areas as needed), to *design* a program. For the *implementation and operation* of a program, sometimes a different cross-functional team is put together based on the desired expertise, influence, and capabilities.

It is important to identify all the groups and individuals that are potential stakeholders in the planning phase. Each may have a distinct interest in identifying the trade secrets, determining value and risks, establishing the ROI, and choosing compliance policies. Regardless of who is directly involved, engagement and buy-in from senior management will be critical. Following the design phase, this same or a new set of stakeholders may also have a role to play in implementation, compliance, monitoring, and enforcement.

The decision of who should be involved in planning and, later, implementing a protection program will vary across companies and industries.[16] The team members bring not only

---

coordination between the legal requirements of patent and trade secrets law as well as strategic consideration of what information will be claimed under a patent application and what will be retained as a trade secret. For example, some companies will face the business need to make disclosures of information they hope to patent to potential sources of funding under nondisclosure agreements but will need to evaluate the potential impact of the timing of even protected disclosures on their ability to later secure patent protection for the information that has been disclosed. *See* Helsinn Healthcare S.A. v. Teva Pharms. USA, Inc., 139 S. Ct. 628 (2019) (holding that the sale of an invention to a third party who is obligated to keep the invention confidential may place the invention "on sale" for purposes of the Leahy-Smith America Invents Act, which bars a person from receiving a patent on an invention that was "in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention").

16. These functions can be in separate departments or personnel or, especially in smaller companies, may be performed by management generally. In certain companies, the titles of relevant individuals could include Chief

different perspectives, but different expertise. For example, an HR manager will consider the interplay of the program with any existing or planned employee restrictive agreements, or whether employee surveillance as a protective measure may be improper or unwise. Counsel will consider the interplay between trade secret, copyright, and patent protection. Licensing personnel will consider the potential value of information in existing and planned licensing transactions. Transactional personnel will consider the impact of protective measures on assets that are being acquired and on managing information that may be shared or spun off as part of a transaction. Finance personnel will be focusing directly on the cost and impact of protective measures on enhancing asset value. Information technology and security personnel will bring expertise in existing programs and the availability of additional resources.

Organizing teams to manage trade secret information should not focus simply on team members whose primary focus is internal. Some functional areas—such as marketing, sales, public relations and communications, supply chain and purchasing, patent procurement, and regulatory compliance—inherently involve disclosing information to the public or sharing information with third parties. Some research and development (R&D) organizations have close relationships with universities and may be parties to grant arrangements that require disclosure of some information to the university or the government. Without buy-in from these functional groups and leaders and working out measures that allow these functional areas to do their work, implementation and compliance with a program to

---

Executive Officer, Chief Financial Officer, Chief Information Officer, Chief Information Security Officer, General Counsel, Intellectual Property Counsel or Manager, Chief Compliance Officer, Chief Risk Officer, Chief People Officer, Chief Technology Officer, and Competitive Intelligence Officer.

control and manage the flow of assets identified as trade secrets can be difficult.

Bringing complex teams together to design and implement a program will require that assessments and decision making are not siloed, but instead are centralized or reached by consensus of the whole. While identifying stakeholders is the critical first step, outlining a centralized governance model, how decisions will be made, and how these stakeholders will each effectuate their roles and responsibilities within the team is another important step.

3. Identify the company's trade secrets

Whether to enumerate or create an "inventory" or "list" of trade secrets and, if so, to what degree of specificity may be one of the more controversial design decisions. Some companies proactively catalog and manage detailed portfolios of trade secrets; this approach can result in broader business benefits, insights, and risk mitigation. For example, Taiwan Semiconductor Manufacturing Company Ltd. (commonly referred to as TSMC) has been internally registering trade secrets since 2013, growing to a catalog of over 140,000 trade secrets by 2021.[17] For some businesses, however, building and maintaining such a corporate-wide trade secret registry may be seen as daunting and overly resource-intensive. Some companies can create an inventory or list without disproportionate administrative burden.

17. Jacob Schindler, *TSMC Has Catalogued More Than 140,000 Trade Secrets Since 2013, Company Says*, IAM (Oct. 1, 2021), www.iam-media.com/trade-secrets/tsmc-has-catalogued-more-140000-trade-secrets-2013-company-says. Such a registry is embedded in the company's invention and disclosure process, designed to capture and record a more expansive portfolio of intellectual property beyond patents. Developers at TSMC are encouraged to focus on the commercial value of information they are creating and on why it gives a competitive advantage over those who do not know the information.

Many companies may see the need for, and benefit from, some system of tracking that does not necessitate or create excessive administrative burden.

That said, some argue that establishing an inventory of trade secrets in advance of a specific dispute can create business risk because some secrets might be inadvertently omitted from the inventory, potentially impairing a future trade secret enforcement action. Others argue that it is simply an impossible task, particularly for large, multinational companies, to create and maintain a current and complete inventory of trade secrets. These objections should be scrutinized and weighed against the benefits of some form of identification or cataloging that minimizes litigation risk, informs the design team and workforce of what is being protected, and prepares the company to respond quickly in the event that enforcement is required.

Regardless of the mechanics of identifying trade secrets, and whether a formal inventory is prepared, many businesses already have an understanding of many of the key assets they own, at least to enable communication with employees and trusted outsiders about what information is to be treated as a trade secret.[18] When, however, trade secrets are vaguely defined and shared to receiving parties, they are at practical risk of loss, and in any enforcement litigation, the receiving party may be able to argue convincingly that it did not have reason to know that the information should be protected.[19]

Identifying or tracking trade secrets for purposes of designing or managing a protection program usually requires less specificity than identifying trade secrets for an enforcement

18. *E.g.*, Big Vision Priv. Ltd. v. E.I. DuPont de Nemours & Co., 1 F. Supp. 3d 224 (S.D.N.Y. 2014), *aff'd*, 610 F. App'x 69 (2d Cir. 2015).

19. *E.g.*, Scentsational Techs., LLC v. Pepsico, Inc., 13-cv-8645 (KBF), 2018 WL 2465370 (S.D.N.Y. May 23, 2018), *aff'd*, 773 F. App'x 607 (Fed. Cir. 2019).

action. The purpose of the former is to inform the business process designing the overall program, including high-level categories of risk and means to mitigate it. Enforcement litigation, in contrast, requires identification with particularity sufficient to enable the defendant to prepare a defense to specific claims of misappropriation and the court to manage the action, a process subject to defined legal principles and civil procedure.[20] The two approaches are not unrelated, but identifying trade secrets in the course of business operations is generally directed to a larger universe of information and may be less formal than for presentations in the course of litigation.[21]

When managing protection programs, some companies identify categories of trade secrets without enumerating each specific secret. If the category has meaning for the company and its employees sufficient to create a shared understanding of what the trade secrets are, then this may be sufficient, even if more exacting descriptions may be needed for litigation. For example, if the trade secret is related to the operation conditions used to perform a method of manufacture in a particular piece of equipment (e.g., specific temperature, agitation torque, shear level, and residence time) then identifying the trade secret as "the process conditions of mixing in Tank P123" may be enough for purposes of internal management. However, it may not meet the particularity standard of an enforcement litigation since it

20. *Big Vision Private*, 1 F. Supp. 3d at 260–61 (S.D.N.Y. 2014) (disclosures during a corporate disclosure of trade secrets to a third party need not use the word "trade secret" but should do "something" to put the recipient on notice of his obligations related to the trade secret information being disclosed whereas in the litigation itself, the plaintiff was required to identify with particularity exactly what information was at issue in the litigation).

21. *See* The Sedona Conference, *Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases*, 22 SEDONA CONF. J. 223 (2021), https://thesedonaconference.org/publication/Commentary_on_Proper_Identification_of_Trade_Secrets_in_Misappropriation_Cases.

does not reveal what the process conditions are. "Customer lists" is another trade secret identification category that may be adequate for an internal program, as employees will often understand what that is even though specifics—the "list" at issue is this particular portion of a specific customer database—may need to be parsed out in litigation.

In any event, potential risks attach to any level of identification or decision not to identify. If there is litigation, the way that trade secrets have been internally identified (or not) may become relevant. Taking the manufacturing trade secret example from the preceding paragraph, if the enforcement action identifies the trade secret as the specific temperature, agitation torque, shear level and residence time of mixing but ties these variables to a completely different piece of equipment (e.g., a tubular reactor rather than Tank P123), defense counsel will be asking some very difficult questions and likely arguing that the information at issue in the lawsuit was never treated as a trade secret by the plaintiff before litigation.

Identifying trade secrets in the course of business should take into account differences in the type of information being considered. Some trade secrets, by their very nature, can be precisely captured and documented (e.g., the formula for Coca-Cola). Others may be identifiable more generally at a high level but challenging to break down, define, and summarize concisely (e.g., source code or a large data set collected and held by a company). And still others are legitimate secrets developed over time but are harder to define or distinguish from unprotectable personal skill (e.g., a business method to achieve a specific result, such as leadership development or converting marketing targets into paying customers). Some, such as software applications, are inherently fluid, dynamic, and continuously evolving or overtaken by market developments or technical improvements. Notwithstanding these differences in types of trade secrets, the company's focus should be on communicating

to recipients that particular information is to be protected as a trade secret. Procedures can also be established to address questions, both during the relationship and, particularly, when a relationship with the receiving party or employee ends.

Some emerging approaches to trade secret protection leverage new technologies to apply to the process of identification. Software can inspect contents of documents and machine-learning tools can review internal correspondence to help flag particular information as potentially qualifying as a secret. In addition, trade secret registries and other software included in a company's research and development environment can enable engineers to identify and effectively document trade secrets during and after innovation. Registering trade secrets on blockchain could create an immutable, verifiable record of creation that may ultimately strengthen legal enforcement positions.

Regardless of one's view of the relative merits of these approaches in the abstract, companies should consider whether individuals within the organization are already making *their own* rather than *institutional* decisions about what information should be kept secret and access controlled, what must stay internal within the company, what can be shared securely with partners, and what can be put into the public domain. Those who are engaged in designing a protection program should consider these realities. They should consider collecting documentation of existing approaches to protecting information and interview senior management, R&D personnel, and other professionals about what they think is most valuable.

4. Conduct an internal assessment

a. Valuation and business impact assessment

Recognizing the value of the trade secrets informs an understanding of the potential impact to the business of a loss or compromise of sensitive information. That understanding, in turn,

will permit a reasoned judgment about the level of cost—in terms of resources and accepted inconvenience—that is appropriate to secure that information. Valuation for this purpose is not a precise numerical exercise; it is necessary, however, among other reasons, to enable the company to assess priorities. At times there also may be good reasons to determine more precise values, including to justify collateral for debt and investment, establish insurability, and to inform negotiation of merger and acquisition or license transactions. When considering valuation for this purpose, questions to be explored may include:

- *Confidentiality*. What would be the business consequences if competitors or other interested parties saw or copied the secrets?
- *Integrity*. What if secrets are deliberately or accidentally altered or contaminated with information belonging to another?
- *Availability*. What if the secrets were irreversibly lost, deleted, or destroyed?[22]
- *Cost to Develop*. What did the owner spend to develop the trade secrets?
- *Market Value*. What would a willing buyer pay for the secrets?
- *Discounted Cash Flow*. What is the net present value of income that can be derived from the secrets?

b. Risk assessment and management

Once management has aligned on what the company's trade secrets are, then threats, vulnerabilities, and risks can be identified as well. It is important to remember that loss may occur through internal or external actors, and the behavior may be

22. *See generally Sedona Employment Life Cycle Commentary*, *supra* note 8.

inadvertent or intentional. The business should consider these vectors of loss in the context of its unique information assets. This connecting of risks to related categories of valuable assets is important in supporting business decisions on protection measures and controls.

Risks can be both outbound and inbound. Outbound risks include theft by a third party, leakage from the inside (employees taking secrets out the door or sharing them carelessly while employed), loss of the institutional knowledge of a secret (e.g., when employees leave and the secret is not fully recorded or documented), and loss from unauthorized use or disclosure. Inbound risks can include contamination by confidential information from a third party entering the company, including from new hires[23] or from customers, vendors, or other business partners. Potential but ultimately unsuccessful acquisitions often present a high risk of inbound infection, as those evaluating a transaction gain greater exposure to work others are doing. Even completed transactions, where a company is acquired and there is an imperfect record of confidentiality agreements or third-party custodial data, can lead to unwanted contamination.

With the rise of the gig economy, companies face increased inbound and outbound risks when using workers who are not employees, such as consultants, temporary or contingent workers, or workers in shared or coemployment situations (also referred to as "secondments"). Consultants working simultaneously for competitors can present a particularly high risk. Many may believe that they are free to take work they have done for one company as part of their "portfolio" of tools to use for others. Misunderstandings abound regarding what may constitute properly portable "residual" knowledge. Unmanaged risks arise against the background of often inadequate training,

23. *See id*.

policy, contractual clarity, and processes designed to safeguard against them.

If a company's business is international, diligence and understanding of the risks in these other countries (particularly those known for or suspected of not respecting intellectual property) is particularly important to developing protective measures. Companies may interact with a workforce employed by a third-party entity they do not directly supervise or manage. The company should consider the qualifications of foreign suppliers and licensees, comply with required protocols that may be imposed in other countries, and include procedures for securing necessary contractual protections and enforcing compliance, both during and after termination of the relationship. Companies should also familiarize themselves with any formal requirements in the countries of concern for keeping records of trade secrets.

The sheer number and types of risks that could possibly arise with respect to any one of a company's trade secrets or third-party trade secrets in a company's possession, regardless of how significant or valuable they are, may effectively make it impossible to guarantee full compliance and prevention of all potential breaches. Risk assessment and threat profiling can be used, however, to help assess "touch points" with trade secrets and prioritize potential risks of theft, loss, or misuse of such trade secrets and how resources should be allocated to address those risks. Strategic risk assessment and risk management can help a company identify the most vulnerable technology, information, and actors on which to focus policies, processes, or even ongoing monitoring—for example, on particular types of technical or business information, particular suppliers, highly sensitive incubating projects, or particular technological entry and exit points.

Many companies use ongoing enterprise risk management (ERM) tools to identify, assess, and manage a variety of risks that their businesses face.[24] Risk assessment in the area of trade secret protection can be carried out as a separate initiative, but also can be a logical issue to include in a company's ERM program in order to achieve executive oversight and centralized trade secret governance overall, in light of other risks and mitigation strategies. For example, a company may wish to limit who has access to a sensitive portion of the manufacturing floor where equipment is operated and trade secret processes may be visible. Limiting means of ingress and egress to this portion of the manufacturing floor may add physical security of the secret but may also create an operational bottleneck with other production lines or equipment in close proximity. Finding the appropriate balance between these interests becomes a business judgment.

c. Assess company structure, systems, workflows, and culture

An overall assessment of the company's systems to determine what can affect trade secrets (positively or negatively) is important to determine what program components will be both practical and effective. For example, companies should consider their own corporate and management structure, the culture and awareness around confidentiality, any existing functional areas that could be part of a designed program, and how the company, and its competitors, interact with the outside world.

24. Enterprise risk management is a plan-based business strategy that aims to identify, assess, and prepare for risks, dangers, and other potentials that may interfere with a company's operations and objectives, assessing the potential impact of each and methods to mitigate them. This informs a decision about which risks to manage actively, and which risks are not worth the cost of mitigation.

Based on this assessment, a program might be designed and implemented with an enterprise-wide approach, or it could be focused on specific business units or functions within the company. Large companies may consider whether a diversified approach to implementing reasonable measures within the corporate structure is appropriate (at the corporate, business unit, or technology segment levels), with periodic coordination on the reasons for and lessons learned from different approaches. Small or young companies tend to implement trade secret protection on a company-wide basis, reflecting a lesser need for hierarchy. Large companies with varying needs for access to more complicated sets of sensitive information will generally need more detailed policies and protocols, coupled with more intensive efforts at training and compliance.

Assessing existing company systems and workflows is important for at least two reasons. First, some of them can be leveraged in the design and implementation of the protection program. For example, if a company already has hardware and software firewalls and other cybersecurity protections, document retention, social media, and other relevant policies, and locks on the doors, there is probably no need to replace those measures or start over. Instead, these existing systems, policies, and practices can be adapted and leveraged to fit within the comprehensive trade secret management program. Other company functions or workflows may present risks to be evaluated and mitigated. For example, patent application strategies, public relations, marketing, sales, and regulatory reporting compliance, while being critical to overall success of the business, are all areas potentially ripe for inadvertent disclosures.

Like all corporate assets, the scale, types, amount, and location of trade secrets within the company should be considered. For example, for secrets embedded in digital files, what is the general ratio of "secret" data in relation to all digital data of the company? For physical secrets, what is the size and volume of

the equipment? Where are the secrets stored or used (e.g., within the "four walls" of the company or shared with third parties, on what computer systems or in what storage locations, in what countries)? This information can inform decisions on who has access and how access can be controlled and monitored.

Company culture plays a significant role in both supporting a protection program and creating compliance risks. Emphasizing speed can foster engineering and technology advancements, for example, but can deprioritize security and compliance. Similarly, open and collaborative work environments can benefit creativity and innovation and enhance development of a variety of kinds of goodwill but can be more susceptible to trade secret leakage.

Front-line employees are sometimes in the best position to recognize risky situations such as outsiders who are not following visitor protocols, emails inadvertently sent to the wrong recipient, confidential information that is not appropriately marked or stored, or offers to view the trade secrets of other companies. A "see something, say something" culture empowers employees, managers, and leaders to become ambassadors of the protection program. On the other hand, a company whose R&D team, intellectual property team, and salesforce tend to act independently in "silos" may suffer from a lack of awareness, allowing trade secrets to be lost through inadvertent leakage. Another potential risk area is when company personnel with trade secret knowledge have come from academia or are working with academia on trade secret projects or technologies. Academia is generally a group whose orientation is to publish and share information, rather than keep secret and protect it.

B. Designing the Program

Having identified the trade secrets and their business impacts, risks, value, locations, and formats as determined in the

assessment phase, potential risk mitigation measures can be considered, and an overall program designed (or in the case of established programs, refined). This phase will address not only specific protective measures, but also the implementation plan, anticipated compliance efforts, responsible persons, and associated roles and processes. Most importantly, the design (and as discussed below, periodic review and modification) of a program should seek a balance among effective protection, potential business impact, parallel or conflicting business processes and functions, information sharing demands, and legal enforceability.

1. Selecting "reasonable measures" for protecting trade secrets

Regardless of the level of particularity with which a company identifies its trade secrets, the reasonableness of its efforts should always be considered in the context of the totality of the circumstances. For litigation purposes, the core inquiry for determining whether reasonable measures have been employed is often how the information was treated by the company before the dispute arose.

It is difficult to draw useful conclusions from case law because most opinions arise on motions addressing the sufficiency of allegations or evidence, and even where the facts are directly addressed on the merits, the treatment is often cursory. However, some examples of the factors courts may consider are:

- *The size and maturity of the enterprise.* Large, multinational companies are often held to a higher standard of secrecy controls than a small, single-location business.[25]

25. Puroon, Inc. v. Midwest Photographic Res. Ctr., Inc., No. 16 C 7811, 2018 WL 5776334, at *7 (N.D. Ill. Nov. 2, 2018) ("Reasonable steps for a two-

- *The location of the enterprise.* A company located in an industrial, competitive environment with frequent cross-movement of employees may require a different level of security than a company located in a remote, rural area and having a stable workforce.
- *The value of the trade secret.* In general, the greater the importance of the particular secret to a profitable and differentiated product or service, the greater the extent of protective measures the owners will naturally take to reasonably protect the trade secret.
- *The extent and cost of the measures taken.* A judge or jury may be more likely to find reasonable efforts when a trade secret owner implements more robust measures and does so consistently, ensuring that those with access understand what is confidential and how they are expected to protect it.
- *The rationale for the selection of the measures taken and not taken.* Trade secret owners do not have to anticipate all possible risks to the integrity of their information,[26] but control failures will be more readily understandable and excused when the owner can demonstrate that its decisions on security measures were thoughtfully tied to the reasonably anticipated risks.

For a discussion of different size, maturity, and types of companies and trade secrets and how these factors might impact a

---

or three-person shop may be different from reasonable steps for a larger company.") (citation omitted).

26. *See, e.g.,* E.I. DuPont de Nemours & Co. v. Christopher. 431 F.2d 1012 (5th Cir. 1970) (a classic observation that "we need not require the discoverer of a trade secret to guard against the unanticipated, the undetectable or the unpreventable methods of espionage now available"); *see also* Compulife Software Inc. v. Newman, 959 F.3d 1288, 1311–15 (11th Cir. 2020).

"reasonable measures" determination for protecting trade secrets, see Appendix B.

2. Choosing appropriate measures based on the assessment

Based on the assessment of the trade secrets and the business, measures can be chosen to protect particular categories of secrets, taking into consideration their impact value, risks, existing controls, and company functions.

a. Nature of the trade secret

The nature and value of a company's trade secrets informs the selection of effective measures. For example, trade secrets can consist of business information, such as product roadmaps, customer and supplier strategies, marketing, sales, and financial performance targets, which may be adequately protected by general policies and controls. In contrast, technical trade secrets (e.g., often related to the design, functionality, and engineering of a product, how a product is manufactured (process), specialized machinery or specification to achieve a performance outcome) may have longer-term value and require more specific protection policies and measures.

Secrets can be stored digitally or physically. A design drawing can be protected with digital rights management and access governance. In contrast, secrets embodied in a machine, customized equipment, genetic material, process methods, or techniques on a manufacturing floor present different kinds of challenges to ensure adequate protection.

Trade secrets can also consist of methods or processes, compositions or specifications, and apparatuses, with corresponding differences in measures to protect them. For example, method secrets can be recorded in operating procedures, which can be protected in locked drawers and with information

security controls. However, some methods may exist primarily in the memories of those employees who use them and train others to do so (often called "institutional" or "tacit" knowledge). The fact that only a few know the secret may provide great protection from theft but also increases its vulnerability to loss or contamination.

"Negative" trade secrets present unique challenges. Where a company must experiment with multiple paths or iterations before finding the one that works or that works optimally, not only its solution but often also information related to the failed experiments can be considered a trade secret. There is often significant investment in developing what does work (know-how) and what does not (negative know-how). If a competitor knew what paths or iterations did not work, it would save time and money and thereby increase profitability by skipping all the experimentation and resulting failures. These specific negative trade secrets are sometimes improperly confused or conflated with an employee's general skill and knowledge. Negative information, however, is often documented in detail in lab notebooks, as well as in photographs of whiteboards and other data sources that are less frequently subject to corporate retention policies. Considering how and where such information resides and the extent to which it is protectable, and informing those who are aware of research failures that this negative information is itself protectable as a trade secret, may require specific attention in training and the development of special policies and procedures.

b. Different measures and varying effectiveness

Selecting protective measures is one of the most important elements of any protection program. Strong protective measures can not only prevent loss; in doing so they can build and be part of the evidence of value for collateral, mergers and acquisitions, licensing, and other corporate transactions.

Completing a thoughtful assessment and program-designing process can also help identify possible leaks or breaches in a company's security. By identifying and then mitigating these possible leaks and breaches, the entire company (not just the trade secrets) is better protected, which could be important elements of the return-on-investment package when seeking executive buy-in. While this *Commentary* cannot possibly list or describe every possible protective measure, some of them are summarized below, and additional examples and more detailed descriptions are provided in Appendix A.

Policy, process, and awareness are critical to establishing a baseline of expectations and workflows for handling trade secrets across a workforce. Physical security measures (e.g., gates, entrance door locks, safes, restricted areas) are a company's initial line of defense for trade secret protection, in part because they limit access and in part because they signal to employees and others the importance of security. If the trade secret is physical equipment or methods in operation, then campus and building security where the equipment or operations are located may be quite important. If the secret is something easily kept to a small number of those "in the know" (such as a customer target list or a formula that can be programmed into machine operations), then a strict "need to know" restriction is a quite useful, effective, and inexpensive protective measure. In other cases, separating the secret into smaller parts to ensure only a small group of people understand and can access the entire secret may appropriately balance the need to make information available internally against the risk of leakage. However, if every employee on the manufacturing floor, the quality and safety teams, and even third-party vendors need to know the particular secret in order for each manufacturing facility to function, then controls oriented solely around access privileges will need to be augmented by other protective measures such as

strong confidentiality agreements and robust training and compliance protocols.

Contractual safeguards may range from confidentiality marking requirements,[27] document retention policies, social media and electronic device policies, and contracts and policies for nondisclosure agreements and other contracts that govern trade secret information and place the receiving party on notice that particular categories of information are to be protected.

Awareness campaigns can include company-wide messaging, mandatory online training modules, and even live training or podcasts on particular trade secret topics, such as customer information sharing and protecting intellectual property in the supply chain.

3. Process for monitoring, improving the program, and incident response

A thorough and comprehensive program will generally include elements addressing monitoring and assessing the effectiveness of and compliance with the program, making improvements to the program as needed, systems for ensuring that the company promptly becomes aware of incidents of

27. "Confidentiality marking" (sometimes alternatively referred to as "labeling" or "legending") refers to the practice of placing a set of words on a document to signal to the reader how the document and the information contained therein should be handled. Some companies may adopt a scheme to indicate the level of sensitivity or the permitted use for the document, using such terms as "external," "confidential," "highly confidential," "internal use only," and "do not copy." Some companies may implement a particular confidentiality marking scheme for specific types of relationships (e.g., a technical collaboration as opposed to a supplier relationship) and may contractually negotiate for a particular confidentiality marking scheme to be applied. One practice is to include a specific reference to the governing agreement between the parties as part of the confidentiality markings to be applied to each document.

noncompliance, breaches, or loss, and a well-developed incident response plan.[28] These elements may also be factors that courts consider in determining the ongoing reasonableness of protective measures.

4. Integrated enterprise approach: Leveraging existing capabilities and processes and navigating conflicting or competing objectives

Many companies have existing functions and workflows that can be leveraged in developing a program, for example, employee onboarding and ongoing training programs. Usually, companies can add the topic of trade secrets in a way that helps employees understand what the company considers to be valuable and what employees are expected to do to protect it. Another example is document storage in IT systems. A review of the security of information technology systems may reveal an already existing strong system (e.g., passwords, encryption, firewalls, virus and malware protection, and auto backup). In this case, the strength of the system is a measure protecting the secrets, even though it may not have been initially designed solely for that purpose. In all cases, the IT system needs to be maintained and periodically reviewed for adequacy of trade secret protection and updated as needed.

However, additional program measures may still be required based on special circumstances. Carrying through the IT example, should access to files or folders where secrets are stored be limited, and who should administer and control such access? Should the secrets be segregated? If there are

28. *See, e.g.*, Hagler Sys., Inc. v. Hagler Grp. Glob., LLC, No. CV 120-026, 2020 WL 2042484, at *2, *11–12 (S.D. Ga. Apr. 28, 2020) (discussing with approval electronic security measures including tracking network activity as well as storing information on private database and requiring multiple credential levels).

weaknesses in the system, then new measures will require more extensive IT planning, modification, and implementation. If there are strengths, they can be harnessed. Identifying existing functions and workflows to be leveraged in a program can lead to effective protection with minimal business interruption and cost. The company's existing document storage system often allows for granting and withholding permission to individuals on a folder-by-folder basis, for example. Controlling access to sensitive information in the document storage system can be straightforward, with some forethought.

In contrast, some existing functions and workflows can present conflicting goals and disclosure risks. For example, companies communicate with the outside world through press releases, trade conferences, regulatory reporting, and sales and marketing efforts. The purpose and goal of these efforts is to obtain a variety of benefits by getting information about the company and its products out to the public.[29] These efforts can, however, depending on the information and the nature of the disclosure, be in conflict with the secrecy goals of a trade secret program. In developing a program, these organizational conflicts need to be identified so that a proactive plan is put in place to prioritize and intentionally decide among multiple goals (instead of reactive damage control). Engaging necessary stakeholders from the beginning and providing trade secret training to the leadership of these functions can help ensure that competing objectives are appropriately weighed.

Coordination continues to be important where trade secrets at issue relate to products that will be publicly marketed or licensed. The team would benefit from early coordination on the timing and legal impact of any public release: the existence and

29. Popular examples of this kind of technology signaling are patent applications and white papers.

configuration of a product can no longer be kept "under wraps" as a trade secret after the product is publicly marketed, for example; however, new protocols, contractual and technical, may need to be adopted to maintain secrecy over the inner workings of the released product.[30]

5. Information technology and cybersecurity

Technologies for both protecting and stealing trade secrets are constantly evolving in sophistication and availability. In most cases, however, companies already have encryption, firewalls, and other protections in place and only need to identify and mitigate gaps in the system rather than design or implement an entirely new IT security system to address external risks.[31]

Trade secrets need to be accessed by at least some employees in day-to-day activities—indeed, that is how a company derives competitive advantage. On the other hand, the digitization and democratization of these same trade secrets, which typically makes their use more efficient, makes them more susceptible to loss, by enabling their exfiltration through an errant email or on a single thumb drive or contractor's smartphone. In any program, it is essential for decision makers who are well versed in the value of particular information to strike the right balance *for the particular company* between the productivity boost afforded

30. *See, e.g.*, Broker Genius, Inc. v. Zalta, 280 F. Supp. 3d 495 (S.D.N.Y. 2017) (denying motion for preliminary injunction on a trade secret claim where the alleged trade secrets had been disclosed to software licensees under a software license prohibiting copyright infringement but imposing no confidentiality obligations or restrictions on reverse engineering; the case illustrates the potential importance of coordinating the protection of information under a variety of intellectual property regimes).

31. *See Commentary on Information Governance, Second Edition*, *supra* note 5, at 114.

by these powerful digital applications and tools and the risk of inadvertent disclosure or outright misappropriation of *particular* trade secrets. This need has only increased in importance in the wake of digital transformation and remote work environments across companies.

While securing "structured data" in databases and systems using access governance and encryption can be more easily implemented, "unstructured data" (e.g., emails, PDF, PowerPoint, Word, and Excel documents), as well as collaborative communication services such as Zoom, Slack, Monday.com, or Microsoft Teams, which are ever more pervasive in today's communication culture, can often be more difficult to secure. Classification of emails and electronic documents and adding rights-management protection for both internal and external sharing can add additional layers of security to more transient information. Becoming familiar with the security options and tools afforded by new technologies is helpful; failing to take advantage of such protections, when available and in wide use, has been found in some cases to be a failure to take reasonable measures to protect trade secrets.[32]

6. Managing and sharing information with third parties with a need to know

Certain businesses thrive or grow with the assistance and collaboration of third parties. These third parties might be key vendors or suppliers, part of R&D and the innovation process, cloud service providers, distributors, licensees or franchisees of the technology being protected, customers, or regulators and

32. *See, e.g.*, Smash Franchise Partners, LLC v. Kanda Holdings, Inc., No. 2020-0302-JTL, 2020 WL 4692287 (Del. Ch. Aug. 13, 2020), *vacated in part* (Del. Ch. Oct. 8, 2020) (finding that failure to use tools to restrict access to Zoom conference calls and to keep track of attendance evidenced failure to take reasonable measures to protect secrecy of information disclosed on the calls).

certification auditors. Protective measures adopted and designed for a company's own workforce usually are not applicable and may not be fully appropriate for these partners and third parties.

Program design should include measures that have been adapted to these third parties and the unique risks that information sharing entails in these relationships, taking into consideration any professional confidentiality obligations, legally required disclosure obligations, and other relevant factors. For example, the risk of theft by an auditor, legal counsel, or an investment banker is usually substantially different from the risk posed by an acquisition target, supplier, or customer with technology or products in the same industry.

When arms-length third parties who are not otherwise bound by professional obligations seek access to trade secrets, confidentiality agreements, pre-engagement due diligence regarding such third parties and their information security practices, and restricting exposure to only those secrets necessary for the relationship are widely used measures to control use and disclosure of shared trade secrets. Pre-engagement due diligence of a "receiving" third party's corporate culture and safeguards regarding its own confidential information can be highly informative. This kind of due diligence can include reviewing the third party's confidentiality policies, conducting public record searches (including searches of litigation filings for claims of violations), and gaining other insights into the counterparty's industry reputation and likely need for or incentive to misuse particular information. If due diligence leads an owner to believe the corporate culture and safeguards used by a third-party seeking access to the trade secret owner's information are lax even in regard to its own information, it is not realistic to believe such company will do well protecting trade secret information of a third party. The key is to learn this pre-engagement so that controls and protection can be implemented (such as security

controls, disclosure limits, protection requirements, and the like in contracts and in disclosing company's internal protocols with this third party). Conversely, when the receiving party's internal policies seem to be both sound and actually enforced, agreeing that information the trade secret owner discloses will be handled in accordance with the receiving party's existing policies may be appropriate and practical, as it will be an approach the receiving party is already following.

The terms of some protective measures when sharing information with third parties will likely be driven by the secret itself. For example, if a licensee is provided a "black box" for a key portion of the manufacturing process,[33] the contract may prohibit the licensee from opening it and require that the licensor, not the licensee, make any necessary repairs. Another practical control is to embed protection inside software code that contains trade secrets to prevent the code from being copied or downloaded on an unauthorized machine.[34]

In many cases it may not be necessary for the trade secret owner to transfer information to the receiving party's premises or computer system; information can be made accessible through use of a secure electronic site allowing the receiving party to access, but not download, information stored on the trade secret owner's computer system in a virtual data room. Technical resources may even be set to track the identity of user accounts accessing the information, a useful feature in monitoring compliance.

---

33. *See infra* discussion at Appendix A, Part C.

34. This kind of protective measure is an example of a measure that should be protected as much as the trade secret itself, since it will provide a road map to the secret being protected and potentially the key to unlocking its protection.

7. Adding new business processes or systems

Depending on the company's trade secret assessment or review, it may be necessary to develop and implement new "systems" to adequately protect the trade secrets at hand. For example, a company with an "open door" practice may need to establish a sign-in procedure for all visitors and deliveries, with a visitor log, name tags, escort requirement, express prohibitions on mobile phones or cameras in certain areas, or the like. A company that previously shared all contacts and customer prospects or technology advancements company-wide may determine that it is more appropriate to limit disclosure of this kind of information to a smaller group of individuals or add additional protections to the information shared. Many of these kinds of measures provide good protection and are not expensive to implement, but they may cause friction to those excluded from the knowledge sphere, or compliance resistance from those who prefer the less restrictive or prescriptive way of doing business. Leveraging HR in designing these measures, communicating the measures and the rationale to employees, and driving compliance (including senior managers who "lead by example") can help ensure success of the modified program.

8. Consider the stakeholders and likelihood of compliance

As a protection program is coming together, it is important to check back with the groups and individuals identified as potential stakeholders in the assessment phase. How will the measures being considered for adoption impact these stakeholders and their ability to perform their business function?

If suggested protection measures are too complicated, harsh, or cumbersome for regular operations, staff are likely to ignore or work around them in their day-to-day work. For example, implementing cumbersome or restrictive IT structure and requirements may result in numerous "shadow IT" data transfer

systems that become difficult, if not impossible, to track and manage. Employees might create their own data repositories with confidential and trade secret information that is easily accessible to them for their daily work, creating multiple copies of this sensitive information in places where access is broad or protection is light. Or employees might turn to a publicly available app or cloud tool to facilitate a team project because it is easier for their team to collaborate and share information. These types of publicly available tools can be fraught with ownership and confidentiality issues, in addition to cyber risks. Failing to consider the day-to-day practicalities and the needs of employees to perform their jobs when choosing and finalizing measures can doom the ultimate success of the program.

Consider as well the needs of stakeholder groups who have different objectives, such as marketing, R&D, and government compliance, but who may have access to the same trade secrets. Can the measures be adapted to work for all stakeholders and still provide the protection needed? Can the same measures be adjusted for these different groups' compliance? Or should different measures be adopted for them? When conflicts arise, such as when one group within a company seeks patent protection while another group believes trade secret protection is more advantageous, or one group believes that making public disclosures at a trade show is necessary to enhance a market edge while another group is concerned about the timing of the disclosure, how will conflicts be resolved?

Even if it requires more effort or changed workflows, working to understand and manage such issues should result in a better overall program as well as buy-in and compliance from these stakeholders.

9. Identify the responsible persons

Those accountable for implementation and compliance of the program should be clearly identified and made aware of their responsibilities. This is particularly important when multiple company functions, which may include HR, IT, internal audit, and intellectual property, are involved in the program, its measures, and implementation.[35] Some companies have a designated officer filling this role, while others layer this responsibility on other company leaders managing risk and compliance. As with other phases of the project, attorney-client privilege issues should be considered, along with the question of whether design and management of the program is primarily a legal function or a business function.[36]

10. Consider the costs to the company

Companies should identify and, to the extent possible, quantify the anticipated costs to the business caused by the program. Costs include out-of-pocket expenses needed to develop and deploy each of the protective measures; additional headcount that might be needed to implement and monitor controls; the expenses and distraction caused by ongoing compliance; the cost to the company in operational efficiency, throughput, or innovation; and the costs of potential enforcement against noncompliant employees, suppliers, or other third parties. Restrictions on internal information flow may inhibit the business's operations or growth, which should be factored in as well.

If the costs and risks are determined not to be reasonable, consider whether changes to specific measures or the program

35. *See supra* Section III.A.1–2.

36. *See supra* Section II.C (Attorney-Client Privilege and Business Records: A Double-Edged Sword).

overall can facilitate a better balance between adequacy of protection, risk, and cost.

11. Will the program be considered "reasonable measures" and stand the test of time?

When the chosen measures and overall program are nearly complete, it is important to take a step back and consider whether the trade secret owner can frame a reasonable argument and rationale that the program is reasonably adequate, under the owner's particular circumstances, to protect the security and confidentiality of the secrets. If so, the trade secret owner has likely taken "reasonable" measures to protect its information.

Keep in mind that reasonable measures do not mean "all possible measures." Recall that the fact-specific analysis of the "reasonableness" evaluation in litigation requires consideration of the totality of the circumstances and is always considered in hindsight. The core inquiry is whether the measures were appropriate against the backdrop of the risk of loss and the perceived value of the information within the context of the specific company.[37] This is a good time to reevaluate the overall balance among the protection of the secrets, the ability of the company to operate and achieve its business goals, and the relative costs of implementing the program versus any potential loss of the secrets.

37. Xavian Ins. Co. v. Marsh & McLennan Cos., Inc., No. 18cv8273(DLC), 2019 WL 1620754, at *5 (S.D.N.Y. Apr. 16, 2019) ("Each owner must assess the value of the material it seeks to protect, the extent of a threat of theft, and the ease of theft in determining how extensive their protective measures should be." (quoting the Congressional Record for the Economic Espionage Act of 1996, 142 CONG. REC. S12213 (daily ed. Oct. 2, 1996) (Managers' Statement for H.R. 3723, the Economic Espionage Bill))).

Regardless of what measures are ultimately selected and implemented, starting and then making continuous improvements can enhance the safeguards and increase the likelihood that they will be found to be both successful at preventing loss and "reasonable" in the eyes of the law.

IV. IMPLEMENTATION AND MAINTENANCE OF THE TRADE SECRET PROTECTION PROGRAM

A. Implementing the Program

No matter how good a program is on paper, it cannot by itself protect trade secrets, let alone withstand "reasonable measures" scrutiny, if it is not properly implemented and maintained. Indeed, a common defense argument in an enforcement proceeding is to point out anything in a program that was adopted but not implemented consistently.

As discussed above, a successful implementation roadmap requires buy-in from key stakeholders and management, and one way to ensure their endorsement is to fully inform them of the business and operational benefits and articulate a clear return on investment (ROI).

1. Implementation planning and execution

An implementation plan should provide clarity on the "who," "what," "when," and "where" needed to perform the implementation and what constitutes completion. Implementation usually involves rolling out individual policies, training, and awareness campaigns, ensuring necessary business processes are in place, and installing any new technical or physical measures. Some programs may be better implemented in stages, while others should be introduced all at once. If the program is being implemented in stages, attention should be paid to the potential implications for an enforcement proceeding arising out of activities or occurrences during the staged implementation as well as comparisons between the "new" program and earlier measures that may be being litigated.[38]

38. *See infra* Section IV.B.3 (Maintaining Compliance—Monitor and assess compliance).

Once execution begins, progress should be monitored, and impact should be measured.[39]

2. Program launch and communication

Communicating the adoption of the program or the individual policies to all affected persons and companies offers an opportunity to set the tone from the top (and not just from counsel) regarding the value of the program and to gain participation and engagement from every employee and affected third party. This communication may be tailored for various audiences. For example, in a small company that does not generally share information with outside third parties, the launch may consist of a simple email message. However, for a large, multinational corporation with several divisions and locations that work with many third parties in high-risk regions, there may be several different communications to different audiences. No matter who the audience is, a good communication effort can drive effective compliance.

Program "launch" may be a misnomer in that most companies already had some safeguards in place to protect trade secrets. In many cases, a well-considered program such as described in this *Commentary* will be primarily in the nature of enhancement and refinement to prior approaches, offering the added benefit of visibility into the return on investment of the adopted measures. Companies would be remiss in ignoring ways in which they are building on prior approaches to protect and ultimately manage their trade secrets, and they can often benefit from recognizing any existing measures as well as emphasizing the business advantages of new measures and any refinements to existing measures. Otherwise, the program can

39. *See id*.

come to be seen as simply one more set of "legal homework" rather than a value-enhancing tool.

3. Training and awareness

Training and awareness should be the initial focus of any program launch, particularly where the program is aimed at changing behaviors among the workforce. Designing rules and processes in a vacuum, without a dedicated effort to drive and sustain broad adoption, quickly risks unraveling the program. As with the communication plan, consideration should be given to tailoring training for the various impacted groups. For example, if the program includes a new process for logging and escorting visitors to a site, the employees who will be receiving the visitors most likely have no need to know what the trade secrets are but do need to understand the process being implemented and the importance of compliance. However, at this same company, the persons who will be meeting with the visitors and presenting information about the company and its technology do need to know what is and is not a "trade secret," and therefore, what information can be disclosed to these visitors and what "marking" or other identification processes are required, either by the program or by applicable third-party contracts. Training and awareness initiatives should be repeated at appropriate periods to ensure the measures and processes remain effective.

When third parties are part of a program, companies need to decide whether to direct any training to these third parties. This decision may depend on the scope and value of the trade secrets to which the third party has access as well as the nature and duration of the relationship. For example, a licensee of process technology who will be operating a facility using that technology probably has access to a large amount of valuable trade secrets, and targeted training may help reduce the risk of leakage or other misuse.

4. Update and integrate into business and legal processes

Programs should embed policies into existing business processes where possible to drive high levels of adoption and ensure process discipline. For example, it would be desirable to reference the "need to know" policy from the company's trade secret program document when describing the process it uses for deciding which employees will be granted access to which trade secrets, or when explaining how a new work-from-home protocol is supported by the network safety and security measures. Implementation plans should try to anticipate these issues and plan accordingly. Working with the right stakeholders (e.g., IT, HR, or specific managers) to integrate security measures into the overall, regular business workflows will help with ongoing compliance. A compliance and enforcement program can reinforce proper implementation.

5. Update physical and IT infrastructure

Some programs will require physical installations or implementation of additional technological tools and processes, for example, locks on file cabinets or storage rooms, barriers (e.g., gates or locked doors) to entry in sensitive areas, computer hardware (such as firewalls and redundancies), or additional password or authentication protocols. Distraction or loss of productivity while such installations are deployed are best minimized with good preplanning and advance communication or training.

6. Document the program and implementation

Thinking ahead to enforcement, efforts should be made not only to document the program itself, but also its implementation. An effective program may include components that remain in place for a very long time—having a record of when

and how the implementation occurred may be important to demonstrate in enforcement proceedings.[40]

B. Maintaining Compliance

Ongoing compliance and enforcement, as well as periodic review of the program's relevance and effectiveness, can be as important as the program design and initial rollout. Building a culture of familiarity and compliance with a company's program, enforcing protections against breaches when necessary, and regularly monitoring, measuring, and enhancing the program over time can all be vital not only in demonstrating in an enforcement case that a company's trade secret protections were reasonable, but—even more significantly—in reducing the likelihood that trade secrets will be lost, stolen, or disclosed in the first place.[41]

1. Culture of confidentiality and compliance

Developing a "culture of protection" can help to sensitize the entire company (management and staff) to the importance of protecting the company's most valuable information. It can also help people more readily recognize risks in particular situations

---

40. *See supra* Section II.C (Attorney-Client Privilege and Business Records: a Double-Edged Sword).

41. This is not a hypothetical risk. Consider this example drawn from a real-world case: A CEO found a person in his company's conference room after 7 p.m. downloading the company's confidential information. After dealing with the situation and upon investigation, the CEO found out that the person had gained access to the company's offices, walked around taking pictures, and then set up in the conference room where he worked on his computers for hours before being confronted by the CEO. Not one person in the company asked him who he was or what he was doing. Clearly, this company did not have a "culture" of confidentiality or good compliance with its policies—which were reported to require all visitors to sign-in and be escorted and were prohibited from taking pictures without permission.

and to report or take other appropriate and timely action. A confidentiality culture can be built in ways similar to other company cultures, such as physical safety and legal compliance (e.g., relating to securities laws, Sarbanes-Oxley Act compliance, product safety, ethics and anticorruption, and quality requirements). Accomplishing this involves setting the tone at the senior management level, promoting company-wide buy-in, taking thoughtful, affirmative steps to implement policies, and continuing to nurture and message the importance of the issue and the company approach among managers and staff. This is often done in conjunction with HR through training, regular communications, positive reinforcement, and other strategies to build a collective and pervasive appreciation for secrecy and protection.

2. Encourage and facilitate compliance

Periodic communications and reminders, additional or refresher training, and a "secrecy" performance metric in employee reviews can help encourage compliance. So can performing occasional internal "audits," even informally (e.g., conducting a walk-around to determine who is complying with the "clean desk" policy, what desks and file cabinets are locked, whether whiteboards contain confidential information, etc.), and reporting the aggregated results to the entire company (as well as privately counseling those not in compliance).

Facilitating compliance is a slightly different concept. Care should be taken to ensure existing company goals, directives, policies, and practices do not conflict with the new or refined policies and procedures of the program (or vice versa) or create situations where employees become unsure about priorities or their ability to comply with both policies. Coordination of policies may be necessary. For example, a new document retention policy might be issued that could put records of trade secrets at risk for destruction, or office renovations might make it more

difficult to keep confidential information out of sight of visitors. Policies to promote the filing of patent applications or to heavily reward only those applications that are granted (thereby potentially encouraging inventors to add more disclosures in the specifications, e.g., performance or process data, in an effort to bolster the likelihood of issuance of particular claims) may limit the long-term ability to claim particular information as a trade secret. A workforce that begins or stays working remotely can present special difficulties in protecting the company's secret information and may require new approaches to making information securely available offsite. New risks or obstacles to compliance need to be assessed; in some cases, new solutions may need to be designed to adapt to changed circumstances.

While there is no one-size-fits-all approach for implementing these compliance elements, special attention should be given to the teams or persons responsible for compliance, attorney-client privilege issues, and whether business records should be purposefully created and recorded regarding the periodic compliance efforts, findings, and any responsive actions.

a. Internal issues and variations

Ensuring the workforce understands what is secret and how to protect it is an essential aspect of compliance. Not every employee or contingent worker, however, may need to know the same degree of detail about what the company desires to maintain as a secret. This may depend on the nature of each of the staff's roles and responsibilities with respect to the products and services in which the trade secrets are embedded.

For example, in a chemical manufacturing process for manufacturing X product, the marketing, sales, finance, and even the shift operators running the software to make product X should know that the process for manufacturing product X generally contains one or more of the company's secrets; while

other members of the technical staff such as process engineers and chemists may need to know much more detailed information about the secrets associated with manufacturing X; such as, for example, the importance and secrecy concerning each of the critical steps, conditions, or ingredients used in the process. If the trade secrets have been identified with some degree of detail, then this type of sequential need-to-know instruction may be more easily accomplished than if the trade secrets involved in manufacturing product X have not been identified to such a detailed level. In other situations where little detail has been shared, compliance may be effectively achieved by informing all staff that the manufacturing process for product X contains trade secrets and the only information that staff may disclose to others is what is disclosed on the company's webpage concerning product X.

Different "groups" or divisions may require different approaches to encouraging compliance. Some companies may want R&D personnel to collaborate internally across product lines, for example, in efforts to improve or discover new processes and products, while others may direct that R&D personnel focus on only one product. Similarly, the purchasing department may need to know specific aspects of current or planned trade secrets to acquire the correct raw materials, tools, supplies, or services but may not need to learn about manufacturing processes, other than to estimate the timing of needed supplies. One group within the company may be encouraged to be open within the company's four walls or within certain protected third-party relationships (e.g., a joint development partner under a nondisclosure agreement), while another group might be given very strict rules regarding disclosures internally and externally (e.g., purchasing may be aware of trade secrets related to raw materials, but it may be prohibited from making any disclosure to a third party without a supervisor's prior approval). Each of these choices may be appropriate for a particular

company and particular trade secrets—but the decision of how to manage particular information needs to be made as part of an overall strategy, rather than as a "catch-up" decision.

Despite best efforts in the designing and implementation stage,[42] a company may come to realize compliance is suffering because the measures' requirements are too complicated, restrictive, or cumbersome. If this happens, the stakeholders and program leader should consider whether changes will improve compliance and still adequately protect the secrets, or whether the measures are necessary and worth the extra effort.[43] The decision needs to be carefully communicated to the relevant stakeholders and those who will be operating under the program.

b. Third-party issues

Companies need to decide whether contracts alone provide adequate protections for trade secrets entrusted to third parties, or if the company also needs to encourage or monitor compliance in specific ways. For supply chain partners, many companies will want to impose specific requirements (e.g., individual confidentiality agreements from the third party's employees, training for the third party's staff, segregation of the company's secret information, or periodic compliance audits).

Licensees and collaboration partners present related but different risks. Some licensed information can be at the heart of a company's competitive advantage; so can some information presented as part of a collaboration. The contracts for these relationships should typically include multiple protective provisions (e.g., confidentiality, limited use, nontransfer or nonassignability, termination rights after a change in control, audit

42. *See supra* Section III.B.2 (Choosing appropriate measures based on the assessment).

43. *See infra* Section IV.C (Periodic Assessments and Improvements).

rights, and dispute resolution provisions). For collaboration partners, there is added complexity, since technical people from more than one company will be working together. This can also happen in a more limited way as a part of know-how transfer to a licensee. The counterparty may want to disclose and discuss novel discoveries or ask probing questions due to curiosity or a desire to further the project's goals. In any case, these situations are fraught with the potential for unintended disclosure and therefore need careful management. Encouraging and monitoring compliance in these relationships can involve a delicate balance between protecting secrets and meeting the objective of the contract and the parties.

Attention should also be given to the question of whether a supplier or other third party to whom disclosures will be made will in turn have a business need to disclose information to others in order to perform under the contract. If so, both contracts and processes will need to be crafted to control those onward disclosures and ensure that those who will receive information from the contracting party become obligated to treat it as confidential. Otherwise, the information may be fatally compromised.[44]

---

44. *See, e.g.*, Turret Labs USA, Inc. v. CargoSpring, LLC, No. 21-952, 2022 WL 701161 (2d Cir. March 9, 2022). In *Turret Labs*, the court affirmed a summary order dismissing trade secrets complaint where plaintiff had authorized its exclusive licensee to grant access to other users to access and use plaintiff's software without imposing any requirement that licensee limit the further users only to those who had entered into agreements to safeguard and not reverse engineer the computer program. The court found that these contractual failings were not overcome by the fact that plaintiff had taken other measures to protect the secrets while they were solely under its control, accepting the district court's finding that the circumstances were akin to "a Plaintiff having pleaded that he locked all the upstairs windows of his house, while remaining silent on whether the front and back doors were left wide open."

If specific notice or confidentiality marking requirements have been agreed to, they need to be communicated and followed to avoid a risk of being found to have forfeited protection.[45]

Contractual obligations to return or destroy confidential information may present some practical implementation issues, particularly at the conclusion of the collaboration. Most confidentiality obligations contain a requirement (either automatic or upon request of the disclosing party) to return or destroy confidential information at the conclusion of the project or termination of the agreement. However, in practice, it may not always be clear exactly when these contracts have "ended" until long after it has occurred. Further, "destruction" of digital data, even by parties acting in good faith, can become enormously expensive, and less burdensome requirements may be appropriate in particular situations (such as a requirement to render certain information "inaccessible through ordinary means"). Companies should be mindful of such clauses and act appropriately for their particular situation.

c. Managing disclosures to government entities

In many industries, occasions may arise where disclosures of confidential information to regulators or government entities may be important or even required. Disclosure can present numerous challenges for companies that want or need to be compliant with government requests for information while at the same time protecting the trade secret nature of that information. The primary challenge is that most government activity is accessible to the public and, under the Freedom of Information Act and various state law analogs, most documents in the

45. Convolve, Inc. v. Compaq Comput. Corp., 527 F. App'x 910, 924–25 (Fed. Cir. 2013). *See infra* note 61 for relevant discussion.

government's possession are susceptible to public disclosure upon request. At least one court has held that the Defend Trade Secrets Act does not provide an exemption from its state's public records law's disclosure requirements, which may mandate that certain disclosures be made available to the public.[46] Further, a governmental agency (or an individual inside the agency) may publish the information inadvertently or even purposefully with little or no availability of recourse to the owner of the information.[47] Thus, the guiding principle, whenever possible, will often be to avoid disclosure of trade secrets to the government.

However, this approach is not always feasible, particularly in the context of government funded projects, government investigations, certain regulated industries, and company referrals to the government for criminal prosecutions of trade secret theft. For example, when seeking government funding for an R&D project (or complying with the government conditions after receiving government funding), it may be impossible to avoid disclosing information that is commingled with some trade secrets. Other examples may include requirements for the submission of performance data, metrics, or safety or other information.

In making disclosures, the company should ensure that it is compliant with the government mandate, regulations, or

46. Fast Enterprises, LLC v. Pollack, No. 16-cv-12149-ADB, 2018 WL 4539685 (D. Mass. Sept. 21, 2018) (holding that the DTSA does not override the applicable Massachusetts public records laws, which mandate disclosure unless the information is "specifically or by necessary implication exempted from disclosure by statute").

47. While the Theft of Trade Secrets Act, 18 U.S.C. § 1905, enacted in 1948, provides for criminal penalties for the disclosure of trade secrets by federal employees except as permitted by law, it does not provide for injunctive relief or civil penalties.

request but not overinclusive in exposing trade secrets not required to be disclosed by law. When trade secrets or confidential business information are disclosed, the company needs to be sure to properly designate its disclosure as such and be prepared to support the designations factually.[48]

In addition, companies may receive subpoenas for witness testimony or documents in connection with regulatory and government investigations in which it is not a target but has relevant information. This can occur in the U.S. and, for multinational companies, in foreign jurisdictions as well. This can be particularly complex for a company in the context of cross-border disputes. Companies should be aware that such disclosures may be subject to disclosure in litigation or in response to requests by third parties and should consider whether particular disclosures can be appropriately limited or designated as not for disclosure.

When a company makes the decision to refer a matter for criminal investigation and prosecution, the company must also carefully consider what information it provides voluntarily or

48. *See* Freedom of Information Act, 5 U.S.C. § 552(b)(4) (the "confidential information" exemption) and (5) (the "trade secrets" exemption, amended by OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524). *See also* Food Marketing Inst. v. Argus Leader Media, 139 S. Ct. 2356, 2366 (2019) (discussing differences between the "Trade Secret" exemption under the Freedom of Information Act, Section 5 and the "Confidential Information" exemption; to gain the benefit of a requested exemption the company needs to be able to offer a factual basis for doing so). *Cf.* Sepro Corp. v. Fla. Dep't of Envtl. Prot., 839 So. 2d 781, 783 (Fla. Dist. Ct. App. 2003) ("[Under Florida statutory law], the failure to identify information furnished to a state agency as putatively exempt from public disclosure effectively destroys any confidential character it might otherwise have enjoyed as a trade secret."). For a further discussion on identifying information as trade secret that may be also useful in connection with government disclosures, see *Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases*, *supra* note 21.

subject to subpoena. In some cases, voluntary production will not be entitled to as robust confidentiality protections as information that is produced subject to a subpoena. The company should carefully review any protective orders in place to determine what, whether, and how its trade secret information will be used and safeguarded during and after the conclusion of the matter. In other circumstances, the government may seek to compel third-party disclosures for its own investigation (e.g., into an automobile safety issue that involves an automaker's secrets) or for a "public purpose" (e.g., the federal government considering compelling disclosure of manufacturing methods of vaccines in a pandemic). The producing party should make similar evaluations of applicable confidentiality safeguards in deciding how to proceed.

In situations where trade secrets and other sensitive information must or, in the judgment of the trade secret owner, should be disclosed to a government agency, various strategies can be utilized to make the required disclosure while still protecting (in a reasonably reliable way) the confidentiality of the secrets.[49] These strategies should be considered and established *before* any such information is disclosed.

The most important considerations in making any government disclosure are understanding (1) the nature and scope of the government request, including whether compliance is voluntary or mandatory; (2) the protective measures in place or that may be lawfully requested by the disclosing party (protective order, confidentiality agreement, or other safeguards); (3) the protocols for securely storing, segregating, accessing, and

49. *See* Elizabeth A. Rowe, *Striking a Balance: When Should Trade Secret Law Shield Disclosures to the Government?*, 96 IOWA L. REV. 791 (2011), for a deep discussion of the concerns of disclosures to the government, case law surrounding private parties seeking to protect the disclosed information, and Professor Rowe's arguments for balancing the competing interests.

destroying the information, particularly if the information is in digital form or on hard drives or other devices; and (4) restrictions on current and future uses or disclosures of the information and the related need for the disclosing party to designate the provided information as being subject to available restrictions.

If the pending disclosure is related to a governmental body in connection with grant funding or a collaborative R&D project involving a governmental body, there are occasions when some governmental bodies will enter into a confidentiality arrangement, which may include a protocol to be followed for confidential disclosures. Such procedures are not, however, always available to disclosing parties.

Many companies identify a select person(s) through whom all disclosures to the government will be made or require that certain persons review disclosures before made. This is especially important in a research or collaborative situation where there are often regular discussions with government representatives that include providing data, reports, and presentations.

Depending on the jurisdiction and applicable law and agency rules, companies can seek reasonable time, safeguards and protocols, and restrictive measures to ensure the information is protected and returned. Seeking confidential treatment for information that is being or has been disclosed to a government usually consists of specifically identifying all information (line by line) in the document sought to be released or disclosed and providing the justification for its confidential treatment. It is rarely acceptable to indicate an entire document is to be treated confidentially; rather each word, graph or sentence that contains the highly sensitive information is marked. The justification for the confidentiality or trade secret designations varies based on the governing law and the context, but it typically requires balancing the disclosing party's intellectual

property rights and the potential loss to competitive advantage if a trade secret is disclosed, and the extent to which the nonredacted information for release satisfies the overarching right of the public to know.

Companies may also be required or may need to consider making filings with state governments. In doing so, companies need to investigate differences between state law approaches to protecting filed information and should not assume that all state laws are the same or are the same as federal statutes. State laws vary, for example, on matters such as when the submitter will be apprised of any request for disclosure, whether the submitter is permitted or required to intervene to prevent disclosure, whether an agency or a court makes initial decisions regarding disclosure, whether a stay of disclosure is automatic pending final decision, whether exemptions are categorical, and what burdens the submitter and the party requesting information must satisfy.[50] Close attention to differences in relevant disclosure schemes may assist a submitter in determining whether to submit particular information at all in particular jurisdictions and how to designate the information if disclosed.

Further, disclosures of information to third parties who may themselves need to make government disclosures should be

50. *Compare, e.g.*, Long v. City of Burlington, 199 A.3d 542, 550–51 (Vt. 2018) (holding that if the *agency* receiving information establishes that it is a trade secret, the information is "exempt" from disclosure since, among other things, otherwise "contractors and service providers may decline to cooperate with the state") and Lyft, Inc. v. City of Seattle, 418 P.3d 102, 115 (Wash. 2018) (construing Washington's Public Records Act not to include a categorical exemption for trade secrets and to require production unless the *filers* establish *both* that "public records disclosure would clearly not be in the public interest *and* that disclosure would substantially and irreparably damage any person or would substantially and irreparably damage vital government functions," and remanding for further proceedings). Both schemes differ from the Freedom of Information Act scheme.

accompanied by guidance to the third parties about how to make those filings in a way that protects the information. Otherwise, the third party may fail to claim confidential treatment, irretrievably exposing the information to the public.[51]

No matter how or why the information is disclosed, taking additional steps to prepare an inventory of what was provided to the government, marking the information as confidential, and providing a cover letter with any appropriate requests and designations under the Freedom of Information Act or other applicable laws is important. This should be done upon each disclosure (not after the fact).

Some companies may, on assessing these challenges and variations in applicable law, determine as a business matter not to voluntarily share particular information in specific jurisdictions, a decision that likely will have business consequences that will need to be evaluated by company strategists.

d. Responsible persons for managing compliance

A company's management of its compliance and enforcement efforts, like the overall management of its program, does not necessarily need to be centralized, as described above. But it is important as a practical matter that all relevant business leaders communicate and coordinate with each other in managing compliance issues to ensure consistency.

51. *See, e.g.*, M.C. Dean, Inc. v. City of Miami Beach, 199 F. Supp. 3d 1349 (S.D. Fla. 2016) (subcontractor's failure to impose confidentiality restrictions on contractor to which it disclosed information had no claim for misappropriation or redaction when contractor filed information with the city without designating it as confidential; failure to designate filing as confidential permitted the city to make the information available to requestors without redactions).

3. Monitor and assess compliance

Regardless of how a company's program may be designed and implemented, it is helpful to have good management systems in place to organize, monitor, and deal with ongoing compliance. Some of these may be electronic and automatic. Others may involve periodic meetings, analysis, or even performance metrics or audits of staff or third parties. Examples of monitoring and measurement activities that can help to ensure that the various elements of a company's program are regularly carried out include the following:

- *Audits.* Routine or periodic internal auditing of controls and employee team compliance with all or specific protective measures can be used. Audits can target several items, e.g., completion rates of mandatory training sessions, physical measures (are the doors and file cabinets locked, are visitors being escorted, are cameras being used in restricted areas), or contracts (are confidentiality agreement requirements being adhered to, are confidentiality agreements with ongoing relationships current or expired, and do they cover the discussions or activities taking place today). These reviews or audits can be conducted in a spot check or comprehensive manner, randomly or routinely, focused on specific measures or all measures. The most important part of these audits or reviews is that there is follow up. If breaches or lapses are discovered, some kind of mitigating or corrective action should be taken or some communication issued to encourage compliance.
- *IT threat monitoring.* Technologies exist today to perform internal and online IT threat monitoring (e.g., unusual download behavior, specific drive or file access, or cyber breaches). Some electronic

technologies can log activity associated with sensitive files or folders (e.g., access, open, edit, save, copy, or sent). Artificial intelligence, predictive coding, and behavioral analytics can be used to identify possible threats to or losses of the company's trade secrets. Some of these technologies are sophisticated and expensive, some less so. Depending on the trade secrets and circumstances, these systems can be very valuable in monitoring trade secrets and flagging risky or suspect behavior or digital transactions. On the other hand, use of these technologies (like most other measures) is not a necessity to have an overall program that provides effective protection, let alone demonstrate that the company took appropriate reasonable measures.[52]

- *Contracts and processes review.* Companies can and should periodically review and update the forms of contracts, employment agreements, and terms and conditions on purchase orders and invoices, as well as the processes (and compliance with processes) required for appropriate reviews of the same before execution to ensure trade secret and other intellectual property rights are protected. Such process reviews also can help maintain conformity of language and terms, which is an important trade secrets compliance element, as well as one relevant to reasonable measures effectiveness. Contracts for a collaborative relationship in which both sides receive and disclose information, especially when the parties are working on R&D together, require careful and thoughtful attention, particularly understanding the technology

52. *See Sedona Employment Life Cycle Commentary*, *supra* note 8.

involved and the way the business and R&D personnel intend to work together with the counterparty, so that the terms of the contract allow for a successful collaboration while also protecting the secrets. Confidentiality marking requirements should be assessed for workability.[53] Companies should also consider, in particular, whether a time-bounded confidentiality obligation (e.g., for ten years) is appropriate or necessary from a business standpoint for particular information, and the consequences for such limitations legally.

- *Metrics (Key Performance Indicators).* Documented performance metrics can be used to measure items such as whether policies, procedures, and records requirements are being followed, the number of breaches or noncompliance incidents, and the understanding, capabilities, and performance of employees in complying with the company's program.
- *Monitoring of third parties.* Due diligence and monitoring of contractors and third-party business partners as to their understanding, capabilities, and performance in complying with the company's program or contractual secrecy obligations can be conducted. Depending on the secrets and the third parties, this can include periodic physical or digital audits of the third party. This can further include a vendor management office or procurement program that evaluates the effectiveness of a vendor's internal security controls before vendor contracts are executed, followed up by annual audits and updates to address new standards and technology.

53. *See infra* Appendix A, n. 61 for further discussion.

- *Trojan horses.* Intentional typos and distinct markings on key documents or code can be used to prove trade secret misappropriation if the document (or portions of the document) shows up in the hands of a third party or on an employee's personal device.
- *Trade Secret Protection Program Testing.* Certification and ongoing analysis of the company's protections can be conducted, including periodic testing and program reevaluation to show that a program is both a policy and a practice. Some third-party certifications can both improve the program and monitor compliance through external certifying audits with formal or informal standards, such as the NIST Cybersecurity Framework.[54] Some of these internal compliance efforts may also augment efforts to demonstrate the reasonableness of the program's measures in future litigation.
- *Data protection systems testing.* Desktop or tabletop exercises can be run to test the company's data protection systems. Examples of this include simulations

54. *See generally* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Version 1.1 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. The NIST Cybersecurity Framework ("Framework") "focuses on using business drivers to guide cybersecurity activities and consider[s] cybersecurity risks as part of the organization's risk management processes." *Id.* at v. Further, the Framework provides a common mechanism for organizations to: "1) Describe their current cybersecurity posture; 2) Describe their target state for cybersecurity; 3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process; 4) Assess progress toward the target state; 5) Communicate among internal and external stakeholders about cybersecurity risk." *Id.* at 2. Ultimately, the Framework is a "risk-based approach to managing cybersecurity risk." *Id.* at 3; *see also* NAT'L INST. OF STANDARDS & TECH., CYBERSECURITY FRAMEWORK, https://www.nist.gov/cyberframework (last visited May 31, 2023).

of trade secret security breaches, hiring "hackers" to try to breach security controls, designating a "red team" and a "blue team" of employees to carry out and defend against a simulated attack, or practicing response procedures in the event of a breach. These disaster response exercises should also address physical or natural disasters such as earthquakes, fire, hurricanes, tsunamis, or even pandemics.

- *Monitoring of publicly available information.* Systems can be established to monitor for disclosures or losses of the company's secrets through periodic searches of the internet, social media, patent applications, and other publications. Establishing routine open-source intelligence searches to capture the company's secrets is a simple yet surprisingly effective way to uncover potential or actual losses—and to help companies reassess whether information they had previously claimed as a trade secret is now known within the relevant industry through legitimate means.

C. Periodic Assessment and Improvements

Change is constant. The trade secrets themselves, their value to the business, the risks of loss, and the effectiveness of measures to protect secrets can all change over time. Indeed, some trade secrets have a short life because a patent is filed, competitors develop the same secret on their own, the secret has been disclosed (purposefully or inadvertently), and many other reasons even if the program is quite sound. With respect to a program and risk mitigation, these changes can bring significant threat of loss. An undertaking to assess, evaluate, and update a company's program on a regular basis, for example, once a year, can be an important step in maintaining reasonable and

effective protections and in prompting compliance on a continuing basis.

As discussed above, special attention should be given to the positions or teams responsible for such reviews and potential program changes, attorney-client privilege issues, and whether business records should be purposefully created and recorded.

1. Assess changes in secrets: their value and risks

Periodic review and assessment of the company's trade secret portfolio (specifically identified or not), as well as the relative value of the secrets is an important item to begin a periodic review. Has the technology, apparatus, product, or business practice changed or been completely replaced? Has the value of it changed (either by increasing or decreasing in value)? Have new trade secrets been created? If so, what is their value? Consider any changes to the company's business strategy, locations, structure, and practices. Do these changes impact the secrets?

Based on an understanding of these changes, an updated risk assessment is the next important item in a periodic review. How have the risks changed? Has the potential impact of the risks, if realized, changed? Has technology (particularly IT and cyber practices) increased or decreased the risks? How do changes in the company's business strategy, locations, structure, or practices impact risks to trade secrets?

2. Review the effectiveness and relevance of measures in the program

With the assessment in hand, the company should review its program's elements and measures, evaluate compliance internally and by any third parties, examine any problems that have arisen (e.g., adaptations to or circumventions of measures, compliance failures, breach incidents, or material trade secret loss). In light of these trade secret, value, risk, and compliance

assessments, a company can evaluate the effectiveness and adequacy of its program to protect the secrets under these "new" circumstances. This evaluation should also include the relevance of each measure. Given certain combinations in the changes, some measures may be found to provide very little protection and therefore can be stopped as irrelevant or ineffective.

3. Adapt, update, and improve the program as necessary

With the assessment and evaluation completed, the company can then make any adaptations, improvements, or additions to the program to protect its then-current trade secrets within the context of the then-current circumstances. Note that this kind of evaluation can result in determining the plan is overkill in some areas (leading to removing some measures from the program), as well as determining that it is lacking in others (leading to entirely new measures being added). Improvements could also be directed to modifying existing measures or wholly focused on compliance with the program that exists.

Some may argue that this assess, evaluate, and adapt exercise (resulting in changes to the program) may open the company up to attack in an enforcement action. Specifically, a defendant may posit that the program should have been designed this way from the beginning, or that taking away a measure destroyed the program's reasonableness. Of course, making no changes to a program once implemented raises a similar risk: that because of changes to the secrets, the values, or the risks, the program was no longer adequate and no longer reasonable under the circumstances to protect the secrets. In light of this kind of Catch-22 situation, assessing, updating, and adapting to *actually* protect the secrets is generally the wiser—and more reasonable—course of action.

If significant improvements (whether implemented at one time or sequentially) in the program are implemented, such as, for example, new rules for working at home and accessing trade secrets, it may be advisable to articulate the rationale for the improvements and why they were not implemented previously. This may be useful in an enforcement proceeding to rebut any defendant challenge that the need for the improvement is evidence that the prior program was not reasonable. Pointing out the rationale for the improvements and why it is being made at a particular time (e.g., we discovered that x safeguard was not as effective as we had wanted and that the new improvement addresses the safeguard) will be better evidence that the effectiveness of the existing program was being monitored and improved. While it shows that the prior program was not perfect, it was reasonable, and reasonable improvements were made.

V. ENFORCEMENT OF THE TRADE SECRET PROTECTION PROGRAM

A company's approach in taking action against noncompliance, breaches, and potential losses can itself be evidence of reasonable measures to protect its trade secrets—or conversely, unhelpful counterevidence if these are not done.[55] Indeed, enforcing protections against breaches when necessary,[56] along with regularly monitoring, measuring, and enhancing the program over time, can all be vital not only in demonstrating the program is reasonable, but also in actually reducing the likelihood that trade secrets will be lost in the first place.

A. Ensuring that the company learns of noncompliance, breaches, and losses

A company can do nothing about an incident of noncompliance, breach, or loss if it does not know it happened. The company should take proactive measures to learn of any such incidents. Monitoring compliance should reveal problems as they arise. Losses can be identified through internal investigations and audits, audits of third parties, regular internet, literature, or patent searches, and software to monitor digital and system transactions. A culture of compliance should lead to "see something, say something" behavior, which might expose incidents or near misses that monitoring alone might not reveal—as well as self-disclosure of mistakes made by an employee.

---

55. For example, allowing computers with an out-of-date operating system and that had not had a security update in three years to connect to a company's network has been cited by the Federal Trade Commission as evidence of failure to provide reasonable protections for confidential customer data. Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 241 (3d Cir. 2015).

56. *See, e.g.*, Pre-Paid Legal Servs., Inc. v. Harrell, No. CIV-06-019-JHP, 2008 WL 111319, at *11–12 (E.D. Okla. Jan. 8, 2008).

B. Incident response

Whenever there is a suspected or actual material lapse in compliance, a breach, or other loss, the company should have a plan in place for how to react or respond. Quick action is helpful and, in some instances, may be necessary in order to (1) prevent additional losses; (2) demonstrate reasonable measures in an enforcement proceeding; and (3) quickly secure meaningful judicial relief such as a temporary restraining order or preliminary injunction.[57] A response plan should provide for: (1) prompt steps to secure the trade secrets; (2) procedures for conducting a comprehensive investigation; and (3) corrective measures, including an evaluation of whether employee discipline or termination or legal action is appropriate.

The exact contours of efforts to secure the trade secrets will vary depending on the situation. For example, it may involve shutting down an employee's or third party's access to the company's facilities and IT systems. It may include wiping any device that is in the individual's control (recognizing, however, that evidence may be lost in the process) or requesting its prompt return. It could also include approaching a former employee or third party to request return of information or equipment, together with assurances sufficient to protect the information going forward. It could involve agreeing on the appointment of a forensic specialist to image and delete or render inaccessible trade secret information, or working separately with such a specialist to analyze usage and access patterns. A full investigation may be followed by one or more of these steps before litigation is commenced.

57. Alamar Biosciences, Inc. v. Difco Labs., Inc., No. Civ-S-941856 DFL PAN, 1995 WL 912345, at *6 (E.D. Cal. Oct. 13, 1995) (4-year delay was inexcusable).

1. Conduct an investigation

Whenever there has been a material or repeated lapse in compliance, a breach, or other incident where there was an actual or potential information loss, an investigation should be conducted. The process should seek to preserve relevant evidence and determine what happened, why it happened, who was involved, whether the breach of compliance was deliberate, inadvertent, or due to a system deficiency, and the nature and impact of the loss. It is often wise to include in-house or outside counsel in any investigation to protect communications as privileged and, if it were to lead to a dispute or enforcement action, establish work-product protection.

Early investigation could reveal vulnerabilities or gaps in the overall program or specific measures that may need updates or improvements. It may provide key information related to compliance and potential gaps or weaknesses in the company's monitoring efforts. Most importantly, the company can make an informed judgment about what, if anything, has been lost, how it was lost, and what to do about it.

2. Take corrective action

Based on the results of the investigation, leadership (often with the advice of counsel) should determine what remedial actions should be taken. Depending on the circumstances, this may range from very modest and discreet steps (e.g., secure the trade secrets and modify aspects of the program), to additional employee training or employee discipline, up to seeking formal remedies (e.g., temporary restraining order or preliminary injunction).

An incident response plan should be followed carefully and expeditiously in the event of a cyber breach or other trade secret theft or loss. Such a plan can be instrumental in dealing

promptly and comprehensively with incidents, as well as limiting and containing the damage.

a. Employee incidents[58]

Employee incidents can range from a serious or a repeated failure to comply with specific security measures (e.g., failure to put away or lock confidential information), to loss or theft of a company computer while traveling, to risky cyber behaviors leading to a breach, to unauthorized download of documents or secrets or transfer of such materials to third parties. Discipline and enforcement actions are similarly broad in range, including general employee reminders, formal and specific reprimands, suspension with or without pay, termination of employment, or the filing of a lawsuit. "Near-miss" emails to all employees for immaterial lapses or mistakes are often effective at both making a memorable impression on the offending employee and a reminder to all other employees to be vigilant.

b. Third-party incidents

If a third party is a strategic collaborator, the incident often needs to be handled diplomatically. In some situations, a gentle but firm reminder that trade secret documents are not to be printed or shared with those outside of the "approved" team can have the intended compliance effect without poisoning the relationship. Providing this kind of reminder is also a significant demonstration of the company's commitment to protecting its information and ensuring compliance. More serious incidents may require engagement of management and often company counsel. The type or level of reaction to intentional breaches or reckless behaviors leading to losses or public disclosures may be used later to demonstrate the value that the owner places on

58. *See Sedona Employment Life Cycle Commentary*, *supra* note 8.

the secrets at issue or on the owner's conviction that compliance with the contract or other measure is important.

c. Legal action

Pursuing legal remedies such as using demand letters, filing civil litigation, or pursuing criminal prosecution may be necessary to stop or seek redress in the event of a theft or misappropriation of trade secrets. Cease-and-desist letters and demand notices are often viewed as aggressive actions and do not always need to be the first reaction to such a serious incident. However, if it is imperative that a behavior stop to mitigate further harm, it may be necessary to quickly escalate the response. As noted above, seeking emergency relief from a court is sometimes the appropriate action. Such relief could include seeking a temporary restraining order or a preliminary injunction or even, where all of the detailed statutory elements are satisfied, pursuing a seizure remedy under the Defend Trade Secrets Act. The exact scope of the remedies available will vary by jurisdiction and factual circumstances.[59]

59. *See* The Sedona Conference, *Commentary on Equitable Remedies in Trade Secret Litigation*, 23 SEDONA CONF. J. 591 (2022), https://thesedonaconference.org/publication/Commentary_on_Equitable_Remedies_in_Trade_Secret_Litigation; The Sedona Conference, *Commentary on Monetary Remedies in Trade Secret Litigation*, 24 SEDONA CONF. J. 349 (2023), https://thesedonaconference.org/publication/Commentary_on_Monetary_Remedies_in_Trade_Secret_Litigation.

APPENDIX A—EXAMPLES OF MEASURES COMPANIES HAVE USED TO PROTECT THEIR TRADE SECRETS

In this Appendix we provide examples of measures a company may consider when developing a Trade Secret Management Program to protect its trade secrets, drawn from collective experience and case law. However, any company's program should be designed based on its unique circumstances dictated by the nature of its secrets, their value, and the risk environment in which the business operates. That a company uses all, none, or some of these measures is not determinative of whether it has deployed "reasonable measures" or efforts to protect its trade secrets. Therefore, this is offered as a starting place, meant to spark discussion and consideration as a program is designed and developed.

A. Policies, procedures, and records

- *Confidentiality, limited use, and material transfer contracts*. Contracts with employees, contractors, joint-venture partners, third-party suppliers, and customers with access to the company's trade secrets, which require confidential treatment, nondisclosure, and use for only specified purposes, are typically a necessary—but not always sufficient—basis on which to prevent unauthorized disclosure and use of trade secrets. Depending on the circumstances and the jurisdiction, it can also be important to specify in such contracts any ongoing compliance monitoring, access, or auditing that the company intends to carry out, including with respect to particular activities such as email, network and internet use, social media, or personal communications. Carefully constructed agreements can themselves be part of a "training" effort by clarifying what the contracting

party's obligations are and what information is to be protected.

- *Third-party diligence procedures and contractual requirements.* In addition to conducting due diligence into third parties who will be permitted to receive disclosures of trade secrets (e.g., tollers, suppliers, vendors, licensees, potential business partners or collaborators, and those evaluating a business for a potential transaction), companies may want to consider special contractual measures with such parties. For example, a company may require (in express terms in the third-party contract) that the third party take certain actions (e.g., limit access to the trade secret to specific individuals, restrict post-disclosure activities of those individuals, provide secrecy training to those with access, allow audits by the trade secret owner, or report apparent violations). Some companies find it helpful to negotiate the right to require individuals at the third party who will have access to information to personally sign confidentiality obligations, or at the least, certify that they have been apprised of the obligations. Some disclosing parties may negotiate audit rights during the relationship or after its termination, require annual training and certification of compliance, and implement closeout procedures for when the relationship ends. Specifying how information will be shared (such as on a shared drive or server controlled by the disclosing party) and how information will be handled once the relationship ends can limit misuse.
- *Confidentiality marking requirements.* Confidentiality markings have been mentioned specifically in some

court cases as evidence of reasonable measures.[60] Consider, however, whether marking every single email, letter, or item as "confidential" is workable in some situations and whether it provides any actual value to the internal company audience. Broad adoption of a confidentiality designation, even for clearly nonconfidential information, may confuse rather than aid employees in understanding how to handle the information the company truly intends to protect. Similar confusion may arise in matters of technical collaboration. If collaboration is expected to span many meetings and both oral and written communications, especially over an extended period of time, requiring specific written notice of what disclosures, oral or written, are to be treated as confidential may initially appear to be desirable, but it can become unwieldy in practice and may lead to a lack of compliance, which can be problematic. Consider the risk to the producing party of agreeing to unworkable procedures or failing to designate information in accordance with contractual requirements.[61] "Escape

60. *E.g.*, Aetna, Inc. v. Fluegel, No. CV074033345S, 2008 WL 544504, at *14 (Conn. Super. Ct. Feb. 7, 2008).

61. It is common for information-sharing arrangements (e.g., confidentiality agreements) to impose some obligations on the trade secret owner to identify information as a trade secret during the course of the information exchange. In these situations, failure to follow these agreed procedures has been found to be a forfeiture of protection. *See, e.g.*, Convolve, Inc. v. Compaq Comput. Corp., 527 F. App'x 910, 924–25 (Fed. Cir. 2013) (granting summary judgment for defendant on trade secret claim where contract unambiguously required trade secret owner to confirm in writing within twenty days that transferred information was confidential and plaintiff had failed to do so); *see also* HCC Ins. Holdings, Inc. v. Flowers, 237 F. Supp. 3d 1341, 1351–52 (N.D. Ga. 2017). Contracting parties will want to be sure that any such

valves" can be built into some contracts, through such means as saying that this type of information "should be treated as confidential, whether or not marked as such," or that information the receiving party "knew or should have known" is confidential should be treated as confidential. Such statements can be backed up by training as well as, in the case of third parties, by looking at what information the third party itself views as confidential in its own business.

- *Post-employment or post-transaction restrictions* with employees, key consultants, departing business owners, business partners, and third parties that limit the ability to compete in a defined way (including restrictions on pursuing particular customers) once the relationship ends can be a strong tool to protect trade secrets. The enforceability of noncompete and related agreements depends on state-specific legal requirements, which are evolving rapidly and range from outright prohibitions on the use of noncompete agreements with departing employees (California, Oklahoma, and North Dakota) to specific limitations both on the permissible content of such agreements and the employees with which they can be used; some states also require specific notice and other formal requirements. The federal government is also assessing potential limitations on the use of noncompete agreements, so this is an area the legal team must review and provide guidance regarding

formalities are workable before agreeing to them and to follow the procedures to which they have agreed.

the latest developments and requirements.[62] Where permitted by law, noncompete and other restrictive agreements should be reasonably limited in scope, duration, and geography in order to be enforceable; specific "consideration" for the agreement may be required by law or may be desirable to enhance enforcement. A contract that imposes sweeping prohibitions may be rejected by courts as an impermissible restraint on trade and held to be unenforceable. A narrower contract may be more enforceable. For example, post-separation restrictions on soliciting the business of particular customers about which trade secret information has been provided may serve the company's needs without prohibiting competition for all other customers and may be more likely to be enforced than a broad noncompete agreement. On the other hand, a contract that is too narrow in scope, duration, or geography may be enforceable but may provide little practical protection to the company. The use of any restrictive covenants as a way of protecting trade secrets needs to be gauged against the changing legal landscape, the nature of the information to be protected, the company's organizational needs, the impact on the party to be restrained, and the public interest. Balancing provisions that are truly designed to protect the company's interest in its trade secrets while allowing the receiving person to

62. The Federal Trade Commission in January proposed a new rule that would ban employers from imposing noncompetes on their workers. The public comment period on the proposed rule ended on April 19, 2023. Press release, Federal Trade Commission, FTC Proposes Rule to Ban Noncompete Clauses, Which Hurt Workers and Harm Competition, https://www.ftc.gov/legal-library/browse/federal-register-notices/non-compete-clause-rulemaking .

continue to make a living or permitting the receiving company to continue to conduct its business without using trade secrets will generally enhance the likelihood of enforceability and protection.

- *Employee or third-party codes of conduct.* A company's expectations and requirements for how employees and third parties should protect and use its trade secrets, and how the company may enforce or otherwise manage compliance, are often expanded upon in more detailed policy and procedure documents. These policies and procedures can be incorporated by reference into the employees' and third parties' legal agreements with the company, sometimes by reference to the company's employee handbook or an employee or third-party code of conduct.[63] Companies should be mindful, however, of the tension between the often-used statement that a "code of conduct is not a contract" and a later desire to point to the code of conduct as a commitment by the employee. The code of conduct can be a useful training and reminder document; it can also be incorporated into a larger contract where appropriate.
- *Document management, retention, storage, protection, and destruction policies.* Document retention, storage, and destruction policies can be practical ways to help restrict the access to and use of confidential information. Examples include limiting the number of copies and numbering and controlling permitted copies, requiring shredding when copies are no

63. *See Sedona Employment Life Cycle Commentary*, *supra* note 8.

longer needed,[64] providing for (and requiring) locked storage for hard-copy documents (individual desks and file storage), observing and enforcing "clean desk" rules (all confidential information is required to be locked away when not in use), and segregating the trade secret into several documents so that if one is taken, the entire trade secret is not taken. When the sharing of trade secret information includes third parties, for example, in a joint venture arrangement or evaluating a prospective business relationship, document management may include storing all shared documents on a server controlled by the disclosing party. Where this approach is not feasible, the parties should agree on processes governing the return or destruction of shared trade secret information at the termination of the relationship or processes for rendering them no longer readily accessible, taking into account the costs of such measures.

- *Electronic Communications and Social Media Policies.* Many companies permit the use of personal devices on company networks and premises. Others prohibit the use of personal devices but permit commingling of personal and business information on corporate-issued devices and cloud storage, including the use of third-party communication platforms such as WeChat and WhatsApp. The approach may differ by region within a multinational company where privacy and data governance laws differ and impose regional constraints on such policies and practices.

64. Some industries are subject to special legal requirements for the preservation of information for specific periods by law or regulation. Those requirements are outside the scope of this discussion.

Whatever framework a company adopts, customized policies and processes should be developed to ensure adequate security and protection of company data, including trade secret information. This framework should also balance the personal convenience of messaging apps with the corresponding lack of visibility and controls from widespread use of such applications on company devices.

- *Human resources and compensation policies and procedures.* There are also practical steps that human resources personnel can take to promote trade secret protection and compliance when employees and contractors begin and finish their work for the company. Offer letters, employee covenants, and onboarding processing can also be used to emphasize both the company's policy and intent not to disclose, use, or learn any confidential information or trade secrets of prior employers, flag potential conflicting confidential information knowledge of a particular employee's former employer, and trigger management of the issue. It can be useful to conduct onboarding training about trade secrets, confidentiality, and the program aspects applicable to the employee. Involving senior managers in the training programs can emphasize the company's commitment to the program (in other words, it is not just "make work"); involving lower-level employees in the training programs can help identify practical challenges or recurring questions. Documenting that staff has undergone training is a useful and often compelling step in enforcement proceedings. Exit interviews and procedures are also useful to ensure that (a) company documentation and equipment have in fact been returned and (b) the employee is

reminded and has acknowledged (sometimes in a separation agreement) his or her ongoing obligations to maintain the confidentiality of the company's trade secrets and other information. Some companies also tie incentive compensation to employees' completion of ongoing training on trade secret protection, or other compliance metrics.

- *Remote work policies.* Increasingly, particularly resulting from the COVID-19 pandemic, employees are working remotely and in less traditional workplaces. This could result in a variety of working situations, from a home office, to the home's kitchen, to a "rent-a-space" desk in a shared work environment, to hotel rooms and hotel common areas, to the road, including cars, trains, planes, rest stops, airports, and restaurants. These changes require a different approach to security and trade secret protection. Companies should consider questions such as: how safe is the internet access available to the employee; who is present when or where he or she is working; how easily could other people see, learn, or steal information; how secure are the employee's devices (computer, phone, tablet) when not in use; should the remote worker have his or her own locking file cabinet or shredder for physical document storage or destruction; should the company collect corporate-issued devices and hard-copy documents via mail or require drop-off, and adapt its exit processes accordingly. Companies can then develop or provide appropriate policies, tools, equipment, guidance, and training to help employees protect trade secrets in these circumstances.

B. Training and capacity building

Trade secret jurisprudence has noted—in finding that "reasonable measures" were insufficient—that a company had failed even to inform employees "what, if anything, [the company] considered confidential."[65] Periodic training, management guidance, and other capacity building for employees, contractors, and even business partners can be a helpful way of focusing attention on the importance of a company's trade secrets and how to protect them, and promoting ongoing compliance. Similar training for outside consultants, temporary or other contingent workers, and workers in shared, coemployment (secondment) situations who have access to a company's trade secrets may also be called for.[66]

Some companies find that active reminders via company network or email notices, in-person events, or even video or social media messaging to be helpful ways of building trade secret protection awareness and compliance, despite the information overloads that many employees and workers experience.[67] Some companies also build websites or other mobile platforms to provide training and policies, compliance requirements, case studies illustrating successful and ineffective controls, and other resources on trade secret protection for employees to access at all times. Regardless of a company's training roadmap, it may be more effective when such efforts are integrated into the company's broader messaging around physical and digital security,

65. *E.g.*, MBL (USA) Corp. v. Diekman, 445 N.E.2d 418, 425 (Ill. App. Ct. 1983).

66. Whenever this *Commentary* refers to "employee," one should consider its applicability for other types of workers who are not in a formal "W-2" type employee relationship with the company, but who are working alongside full-time employees performing similar services and work on behalf of the company, with similar access to the company's trade secrets.

67. *See Sedona Employment Life Cycle Commentary*, *supra* note 8.

environment, health and safety, travel, ethics and compliance, and diversity and inclusion.

C. Physical controls

Physical controls (e.g., locks, doors, walls, or gates) have been a staple in protecting trade secrets for a long time. Physical measures are, simply stated, creating restricted access to trade secrets to those who have a "need to know."

- *Physical barriers.* Campus gates, entrance door locks, visitor management systems (visitor logs, escort rules, security, or visitor badges), and security staff provide a first line of defense by restricting access of the public or nonauthorized personnel to its offices, laboratories, manufacturing floor, files, and records. Similarly, but on a smaller or more specific scale, safes, locked file cabinets, locked storage areas, or specific rooms or areas that are locked further restrict access to the secrets. Other kinds of physical barriers include curtains or screens around portions of the R&D lab or manufacturing floor, and the prevention of mobile phones, cameras, and other recording equipment on premises to restrict the ability of anyone without a need to know to see, record, or otherwise gather details about the trade-secret-protected device, product, or mechanism. Metal detectors can be used to check for unauthorized devices or materials both entering and leaving facilities. "Clean desk" policies (discussed above) and document shredding requirements are another form of physical protection—keeping the information put away on a regular and consistent basis.
- *Data and asset localization.* Another physical security measure that can be very effective for some

companies and some trade secrets is requiring that all assets and data remain on campus. But for many companies and trade secrets, this is not realistic or feasible, due to factors such as employee travel, work performed by employees on client or other business partner's sites, and remote workers who may be working from home or other locations. Employees need to be sensitized to the risks involved in removing assets and data from the company's physical locations and required to take measures to protect it when they do. These measures are most often common sense (locking the car and keeping a close eye on belongings when traveling, not sharing a work computer with other family members if working remotely), and measures commonly used on campus (such as locking a home office or otherwise securing files when not in use when working from home) can be adapted for the remote work situation. Such measures can be useful in protecting certain kinds of equipment, physical components, documents, and other physical embodiments or repositories of trade secrets.

- *Coded ingredients.* Where Occupational Safety and Health Administration (OSHA) and related requirements permit, referring to ingredients by code names—x drops of ingredient A, 2 milliliters of ingredient B—can help preserve confidentiality and limit access to the entire formula.
- *Physical segmentation.* A manufacturing company may benefit from a risk mitigation standpoint by physically isolating various portions of a proprietary manufacturing or assembly process in distinct, separate locations, so that a single breach will not expose all of the related trade secrets. Similarly, when

designing and building a new facility, a company can hire multiple engineering firms or contractors, each responsible for different aspects of the project, which makes them responsible for different trade secrets or aspects of a trade secret. By so segregating, no one firm has access to or knowledge of the entire secret or all of the secrets. A company might also in-source the final or critical part of the assembly or installation for the project to further segregate and protect the trade secret or set of secrets. These tactics and strategies may be on the more extreme end of the spectrum; however, they may be important to consider when building in jurisdictions around the world where intellectual property rights are not well respected.

- *Black Box*. Another strong physical protection is utilizing a "black box" approach. This entails encasing the trade secret to hide it or its critical elements. The black box approach can apply on small or large scales—all depending on the secret to be protected. One example is the operations floor machinery, which can be obscured from view by physical implants such as curtains. Another example is a small component encased in plastic that cannot be opened without destroying the component. The objective is to encase the trade secret in such a way that it cannot be reverse engineered. This technique can be utilized in any number of situations. One company has used this technique to protect a manufacturing process for several decades (rather than patent it for only 20 years). Some companies use this technique to protect the more critical steps of manufacturing processes in countries without mature intellectual property enforcement regimes.

- *Clean Room.* Clean-room procedures are a proactive effort to shield a company's independent development of competing products from future claims of contamination, or improper use of a third party's trade secrets in connection with that development. While clean rooms are expensive, time and resource intensive, and require extensive planning and coordination, they can be particularly helpful where a company's independent development may later be challenged, such as in the context of joint development with suppliers, where a company had previously codeveloped a product or raw material with a supplier and later decides to in-source that product or raw materials. It can also be helpful in the talent recruitment context, where the company has hired several key inventors from a single competitor, who are then assigned to collaborate on developing a competing product, or where a consulting arrangement ends prematurely or disruptively and the company continues with product development.

  In order to be "clean," clean rooms include (1) a specification team comprised of experts who may have knowledge of third-party trade secrets and who identify the functionality or other requirements for the competing product; (2) a screening team that serves to review and filter the information provided from the specification team to the development team, and ensures that procedures are followed to protect information flows in and out of the clean room; and (3) a development team that is physically and digitally isolated in the clean room, is only allowed access to the specifications, and is responsible for the actual design of the competing product. Former employees of competitors and others who may have

> access to third-party trade secret information are excluded from the screening and development teams. Appropriately staffing these teams, maintaining well-documented procedures and records, and ensuring compliance at all stages of the process is important for clean rooms to have the intended safeguard effect.[68]

D. Electronic and information technology security measures

In light of the pervasive risks to electronically stored information and severe consequences of unauthorized access to that information, many companies are presently focusing significant investment and effort in upgrading their information technology systems and infrastructures to deal with and combat the growing risk of cybersecurity threats. Electronic security measures have long been recognized by courts among the "reasonable measures" that can be effective tools for protecting trade secrets and promoting ongoing compliance.[69]

Electronic security controls can be helpful in protecting all kinds of confidential business and technical information in digital form, particularly if these controls are implemented with an understanding of what a company's trade secrets are, where they are held in the company, and what the likely cyber risks for those trade secrets are. Electronic security measures that help to

---

68. *See, e.g.*, Patriot Homes Inc. v. Forest River Hous., Inc., No. 3:05-cv-471 AS, 2007 WL 2782272, at *4 (N.D. Ind. Sept. 20, 2007) (finding a clean room ineffective where months after its creation, "the 'clean room' was still tainted").

69. *See, e.g.*, Revzip, LLC v. McDonnell, No. 3:19-cv-191, 2020 WL 1929523, at *8 (W.D. Pa. Apr. 21, 2020) (denying motion to dismiss alleging failure to state a trade secret claim and explaining that "a reasonable extension of physical security measures is electronic or computer security measures such as password protection").

protect trade secrets and promote compliance can include elements such as the following:

- *Passwords*. Password protection can be established for hard drives of laptops and other machines as well as for access to a system, server, or to specific files, folders, or drives. Password-type protections increasingly involve password strengthening requirements (which may include length, upper and lower case, numerals, and nonalphabetic characters, and renewing on a regular basis).[70] Multifactor identification that uses more than one form of identification (i.e., something you are given plus something you know, or a password plus authentication via text or phone call) is increasingly common, particularly for remote access or for administrative access to systems and data. Biometrics (which may itself be addressed by regulatory requirements, e.g., the Illinois Biometric Information Privacy Act or the proposed federal Commercial Facial Recognition Privacy Act) are also increasingly being used to strengthen access controls.
- *Access controls*. Access controls can be used to limit or segregate use, copying, and transmission of trade secrets by limiting access to certain files, folders, drives, systems, or servers, or by limiting the ability to print, download, alter, or transmit certain files or folders. "Rights Management" technology can be deployed that limits access to authorized individuals only, and so even if content is accidentally shared, such technology will prevent unauthorized viewing

70. Standards for what constitutes a "strong" password change over time. Accordingly, this *Commentary* does not offer specific guidance.

of document contents. The Supreme Court recently determined in the criminal context that the protections afforded by the Computer Fraud and Abuse Act against those who exceed "authorized access" to a computer system do not apply if the defendant had been authorized to access the portion of the computer system from which the alleged taking occurred.[71] As such, some companies may decide to establish separate servers or drives for storing the most sensitive information and restrict access to those locations to only a small number of employees. Companies sharing trade secrets with entities outside the United States may similarly choose to store their trade secret data on servers or drives physically located in the United States so that, among other reasons, access to those locations in furtherance of misappropriation may be found to have occurred "in" the United States for purposes of the Defend Trade Secrets and Economic Espionage Acts.

- *Data loss prevention software*. Data loss prevention software is used by many companies to manage and monitor user activity across systems and networks, and even to and from cloud environments. Data loss prevention solutions can be fine-tuned to look for particular data types and elements and alert when unauthorized use or transmission is suspected. File level activity logging can also be enabled and does not necessarily require the purchase of expensive data loss prevention software. Employees should typically know (and some state law requires notice) that they are being watched closely. But they should

71. Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021).

generally not know exactly how they are being watched, or how monitoring systems work.[72] If they do, they could try to work around the system and find holes. For example, an employee with frequent confidentiality policy violations could be testing the bounds of the system.

- *Encryption*. Encryption of particular files, computer discs, servers, email traffic, and other items can protect company trade secrets even if there is unauthorized access. Enabling and requiring the use of VPN or other encrypted or protected access to the company's system via the internet can provide effective protection for data when not within the protection of the company's four walls.
- *Network segregation*. Network segregation can be used to limit the places where particular trade secrets or other confidential information is held. Also, to reduce risk, trade secrets can be strategically segregated rather than aggregated in a single, centralized network location where a breach could be severely problematic.
- *Firewalls*. Firewalls are used to prevent unauthorized external access to a company's networks, servers, computers, and files.
- *Email filters*. Email filters are used to restrict communications from suspect or spam senders, or with risky or suspicious attachments, files, or web links, guarding against "phishing" and malware attempts. These security services usually also provide filters or protections from visiting potentially risky or suspicious sites (via link or otherwise) that could lead to similar

72. *See Sedona Employment Life Cycle Commentary*, *supra* note 8.

introductions of malware and other attacks that could make the company's digital systems vulnerable and pose a risk to trade secrets and other confidential information.

- *Antivirus and software updates.* Antivirus or antimalware software and regular software updates can guard against cyberattacks, phishing, and other security lapses that increase the risk profile and vulnerability of a cyberattack and could compromise confidentiality.
- *Cybersecurity training*. Cybersecurity training for staff should be considered even when sophisticated and up-to-date email filters and antivirus or antimalware software is in place. Staff that has been sensitized to cybersecurity issues and flags can provide the final line of defense for avoiding risky emails (still one of the most common forms of attack and network compromise) and internet use as well as reporting oddities to be investigated.
- *Protections for travel to insecure locations.* For travel to jurisdictions around the world where intellectual property legal regimes are not well established, or concerns arise around loss or tampering of corporate devices, some companies have plans in place or special "burner" or one-time-use devices on hand in advance to provide traveling employees with the access and information they need for the business purposes of the trip, while protecting the rest of the company's secrets and other information.
- *Automatic backup*. Automatic backup of digital information in the event of a catastrophic event (e.g., weather, accident, fire, or cyberattack) can prevent the loss of company trade secrets.

- *USB drives and other portable device restrictions*. Restrictions on the use of USB drives and other portable storage devices, which may include prohibiting the use of such devices or the blocking of USB ports altogether, can be used to protect information against theft, malware, or device damage (e.g., "USB killers") and unauthorized copying and downloading (even by employees who have no bad intentions).
- *Cloud-based data storage*. Cloud-based data storage raises some potential risks. First, consider the company seeking to move its data storage to the cloud. Due diligence on both the cloud storage provider and the tools to interface with the cloud are key to an understanding of how and where data is (or can be) stored, backed up, accessed, and shared (and thus how it can be protected or lost). A company may believe it has good controls over the internet, firewalls, passwords, encryption, and permissions to file, folder, or storage systems, only to learn that employees can "share" files or folders with anyone who has an email address. Second, companies should consider whether employees' use of publicly available cloud-based storage or group collaboration applications (e.g., Google Drive, Dropbox, Slack, BOX, Monday, Teams, SharePoint, or GLIP) is aligned with company goals and processes. Many employees use these products without permission and introduce significant risk. They may be doing so with the best of intentions to build efficiency for their team or a project, or at the request of an outside party. But few will investigate or understand the privacy implications, ownership rights, and other risks to information shared through or stored in such applications. Similarly, location of cloud servers outside the

United States may raise specific security considerations. Many companies develop policies around the use of cloud-based storage and group collaboration applications for confidential information to avoid these risks.

- *High-risk websites and applications*. High-risk websites and certain domains create significant security risk and vulnerability to trade secret theft, fraud, and espionage, along with opportunities for employees to engage in unauthorized or illicit activity on corporate devices, systems, and networks. Consideration should be given to prohibiting the use of any such websites and applications absent prior approval, whitelisting certain applications (as having been vetted and safe to use), or blacklisting specific applications. If cloud-based storage applications are used, consideration should be given to logging all electronic data transfer activity. Also, companies using such services must be sure that the activity is shut down and the information is removed at the end of any project for which the service is used.
- *Personal device and mobile phone restrictions*. Restrictions on personal devices used for company business under a "bring-your-own-device" (BYOD) policy can be used to control the potential avenues through which trade secrets and other confidential information can be accessed, transferred, photographed, recorded, or used in unauthorized ways. Even if photos or recordings on personal devices have a legitimate business purpose, providing protocols for transferring such recordings to the company's encrypted, protected systems as quickly and as safely as possible can mitigate the risk of use of such devices. Consideration should also be given to

whether and which personal devices (home computers, personal mobile or smart phones, tablets, and pads) should be permitted or prohibited for company business and information. For example, employees may have a desire to "work on it at home" or to use a personal computer with which they have a higher comfort level, even though such an approach could result in leakage of secrets to areas where other digital protections are lacking.[73]

- *Software app whitelisting or blacklisting*. The whitelisting or blacklisting of particular software apps as part of a company's policy can limit the potential risks from untested or unknown computer programs operating on the company's systems. In addition to cloud-based storage discussed above, other applications may create or introduce vulnerabilities to the overall system security. Whitelists and blacklists should be updated regularly.
- *Managing work-from-home risks.* Working from home has become increasingly common and brings additional and different risks to manage. Among other things, companies should evaluate the systems used by remote workers to communicate and access company resources to determine if the connections are secure, whether the data should be encrypted, and whether security systems can effectively support the increased traffic. Companies should consider the value of other potential security measures specific to the circumstances of the remote workforce. Examples of these additional measures include:

73. Similar issues with personal devices are more acute in remote working situations.

prohibiting or restricting the printing of sensitive information, requiring control over hard-copy documents, ensuring that corporate resources are used only by employees and only for authorized uses, discouraging commingling of personal and work-related devices and data, and ensuring appropriate physical access controls are in place in an employee's home.

- *Information retention policies*. Information retention policies, standards, and technology solutions should be considered, not just to comply with any applicable legal and regulatory requirements, but to limit sensitive trade secret information languishing in email storage, file shares, and other repositories. Establishing protocols to purge data when no longer needed can reduce the risk of unauthorized loss or disclosure of sensitive information.

E. Contracts

For contracts, a three-prong approach is often valuable. First, review who has access to information and secrets of the company and determine if valid contracts exist for all such persons or entities. Second, review the terms and conditions of these contracts (and the company's "form" contracts) to determine whether they are strong and appropriate to protect the specific secrets being disclosed in the particular context with the particular receiving party. Consider the possibility that the receiving party is acquired by a competitor or enters into a business transaction with a competitor—does this terminate or alter the information access arrangement? If employee agreements with current employees are inadequate in light of, for example, changes in the employee's access to trade secrets, counsel should be consulted to ensure that any amendments or new contracts will be enforceable, including, for example, whether they require

additional or new consideration. Third, tailor agreements (especially form agreements) to the particular situation and third party. It does no good to have a host of protective measures in an agreement if they are not and, realistically, will not be implemented by a particular third party.

APPENDIX B—EXAMPLES OF HOW REASONABLE MEASURES MAY DIFFER BASED ON FACTORS LIKE THE INDUSTRY, SIZE, MATURITY, AND GEOGRAPHIC FOOTPRINT OF THE COMPANY

Below are some examples of various hypothetical businesses, highlighting how their differences may affect their approach to a trade secret strategy and operational plan. These examples are not intended to be exhaustive and are presented to illustrate a range of business situations and factors for consideration.

Given the great variation in nature of the secrets, their value, and the risk environment from one company to the next, even if two companies are in the same industry or of similar general types, the following illustrative examples should not be misinterpreted to create perfect examples of programs or categories of companies with similar requirements to be compared against either other.

When it comes to Trade Secret Management Programs, no one size fits all.[74]

A. Small technology start-up

A small technology start-up typically has limited resources (venture capital or self-funded) and is in the early stage of

74. Tax Track Sys. Corp. v. New Inv. World, Inc., 478 F.3d 783, 787 (7th Cir. 2007) ("The question here is how much effort to keep information confidential is enough to be considered reasonable? Courts evaluate this question on a case-by-case basis, considering the efforts taken and the costs, benefits, and practicalities of the circumstances. . . . Typically, what measures are reasonable in a given case is an issue for a jury. In some circumstances, however, it may be readily apparent that reasonable measures simply were not taken.") (internal citations omitted); Data Gen. Corp. v. Grumman Sys. Support Corp., 825 F. Supp. 340, 359 (D. Mass. 1993) ("Whether reasonable steps have been taken depends on the circumstances of each case, including the nature of the information sought to be protected and the conduct of the parties.").

product development and commercialization. The team collaborates in an open, information-sharing environment, and the company has little corporate infrastructure or experience with trade secret protection. All team members are involved in all phases of the business, including R&D, product evaluation and testing, and customer and investor meetings. All confidential information is accessible to and shared by the team, and trade secrets have not been specifically identified, classified, or valued.

The team may want to start by developing a trade secret policy and deciding on the roles and responsibilities of team members for implementing trade secret protection protocols. Then the team may determine what resources it can afford to allocate to trade secret protection and develop an operational and financial plan that optimizes cost and risk. Protective measures tailored to the risk will be important, likely focusing on physical and IT security, employee mobility, and third-party interactions. The risk of trade secret loss through employee departures and information sharing with suppliers, potential customers, and partners and through disclosures in the specifications and examples of patent applications may be particularly significant, and so focusing protective measures on contracts, information-sharing protocols, employee exit processes and, where applicable, patent or other intellectual property strategy will be important. The team may also focus on knowledge management—including how to classify, label, share, and print valuable files along with developing role-based access controls.

B. Midsize expanding company

This company has successfully commercialized its first phase of products, is expanding sales volume and geographic scope, and is undertaking new research and development for next-generation products. Additional manufacturing and sales facilities are being built and staffed. The company is developing an internet presence to communicate with customers, third-

party contractors, and suppliers. The company is currently using a general confidentiality protocol for all its confidential information, including trade secrets, and internal access to trade secrets is not highly segmented or restricted. The company is beginning to identify, classify, and value its trade secrets, as well as potentially even documenting negative trade secrets.

The company has a three-year strategic and operational plan that contemplates the need for additional trade secret protection measures. In addition to technical trade secrets, the company is developing business trade secrets relating to special customer and supplier requirements and needs. The company is evaluating new technologies for next-generation products and is also evaluating other companies as potential acquisition candidates. The company finances are sound, but many issues are competing for limited resources.

The company may want to develop a clear business consensus and financial plan for the additional trade secret protections by conducting a risk-benefit analysis, including return on investment for additional protections, both physical and cyber, and whether to move from a general confidentiality protection model to specific identification, valuation, and access restrictions for trade secrets. The company may wish to examine its cybersecurity and trade secret protection culture collectively and find ways to enhance server and cloud security, access, and monitoring. The company may develop training and awareness campaigns on trade secret protection. Business and technology managers may want to consider how they plan to manage the acquisition of third-party trade secrets, and how to integrate and segregate new employees to avoid contamination or infiltration issues. The company may want to examine its document management practices and whether to increase access restrictions for new employees or acquired companies. The company may want to evaluate and clarify the roles and responsibilities of key stakeholders for each aspect of its trade secret

protection program, consider having dedicated positions and resources, and empower stakeholders to address noncompliance issues. If the company is considering developing a patent portfolio, patent efforts need to be coordinated with trade secret protection measures.

C. Data-driven technology company

This company may be in the software, biopharma, on-demand services, or medical device field. The company is established, with mature policies and processes. The company manufactures and sells products and services and is accelerating its business growth to incorporate smart technology employing big data, artificial intelligence, and predictive modeling to complement existing commercial products. The company has robust physical and cyber protection for existing businesses but may desire to modify its program to deal with its new business model, which requires protection schemes for large data sets. The company has not inventoried its trade secrets by business, but some trade secrets cross over from high-profit to lower-profit businesses.

The company may want to conduct a trade secret inventory and classification by product and business to determine risk of loss by licensing or divestiture. The company may also want to decide on trade secret valuation and licensing strategies. The company may wish to invest in additional technology to impose greater access controls, monitoring, and forensic capability around its highest value data sets. With the increasing complexity and diversification of its business models, the company may want to design a dynamic protection plan that can be flexible with business changes but maintain effective controls around data when it is at rest and in transit. The company may want to evolve its employee mobility processes to further protect against data infiltration and exfiltration. As the company builds a larger intellectual property portfolio, coordination of efforts

with respect to protecting information that will be the subject of copyright and patent protection may become even more important.

D. Established, large multinational company

This is a Fortune 300 multinational company, with tens of thousands of employees and contingent workers across the globe, and manufacturing and sales sites in most industrial regions. This company has many business units that share some core technologies, personnel, and functions but generally operate as independent businesses with significant revenues. The company has research and development in multiple locations, and scientists and engineers often work collaboratively and remotely on projects at different locations. The company has a complex supply chain, and in some respects is vertically integrated from raw materials to finished products. The company is publicly traded and subject to global, complex regulatory regimes. The company has a layered management and operational structure, where decisions are made by multidisciplinary teams. Some trade secrets are identified and classified in some business units, but not in all. Some business units are not completely integrated in all company systems, since they have been recently acquired and have different historical systems and corporate cultures.

This company's business case demonstrates many possible trade secret protection circumstances and complexities. The company may want to conduct a business-by-business and location-by-location differentiated assessment of its current physical and cybersecurity systems and third-party contracts to determine strengths and vulnerabilities to be considered for additional resources, management, and prioritization of the most important issues and costs. Information shared in some countries may require particular confidentiality marking or other country-specific legal controls. Or the company may want

to consider making all of its information accessible only on servers it controls located in the United States. Since the company is large and complex, it may be expected to implement a fairly robust system of reasonable measures to protect its trade secrets. Accordingly, the assessment may also include evaluation of trade secret identification and value methodologies, cost of protection methodologies, trade secret authorization and access segmentation, trade secret education and training, and monitoring, compliance, and enforcement protocols, as well as coordination with other components of the company's overall intellectual property strategies and portfolio building.

Although every situation is different, the company may wish to look externally to evaluate how other similarly situated companies in its industry are protecting their trade secrets (e.g., establishing a dedicated chief security officer) and dealing with similar issues, if such guidance is available. The company may wish to evaluate available trade secret protection software, monitoring, and cybersecurity products and services, and may want to avoid operation and research locations that may possess more trade secret risk. The company may want to audit its third-party contracts to determine if they pose a risk of trade secret leakage and there is a need to redesign contracts and protocols to enhance security.

The company may also wish to evaluate the effectiveness of those current employees tasked with responsibility for different aspects of the program and decide whether changes may be needed to effectuate a multidisciplinary team approach. The company may want to evaluate its key trade secrets and revisit how they are classified, valued, printed, stored, transmitted, and controlled at each facility to aid in its decision process concerning additional or remedial physical and cybersecurity methods that it may desire to implement.

Moving the Law Forward in a Reasoned & Just Way