The Sedona Conference Journal®

Volume 26 ❖ 2025 ❖ Number One

Articles

The Sedona Conference®

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

The Sedona Conference Journal®

Volume 26

■

2025

Number 1

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual or semi-annual basis, containing fully vetted Sedona Working Group Series publications and peer-reviewed articles by individual authors on topics related to the mission of The Sedona Conference to "move the law forward in a reasoned and just way." 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 "26 Sedona Conf. J. _____ (2025)."

Publisher's Note

Welcome to Volume 26, Number 1, of *The Sedona Conference Journal* (ISSN 1530-4981, published by The Sedona Conference, a nonpartisan and nonprofit 501(c(3 research and educational institute dedicated to the advanced study of law and policy in the areas of complex civil litigation, intellectual property rights, data security and privacy, and artificial intelligence and the law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way through dialogue and consensus building.

A quarter century ago, *The Journal* was created to showcase the original written materials submitted for discussion at Sedona Conference retreats, limited-attendance conferences that acted as mini-sabbaticals for the nation's leading jurists, lawyers, academics, and experts to examine cutting-edge issues of law and policy. Out of these conferences evolved the Sedona Conference Working Group Series (WGS to pursue in-depth study of tipping-point issues identified at the events, with the goal of producing high-quality, nonpartisan consensus commentaries that provide guidance of immediate and practical benefit to the bench and bar. All of these have been published in *The Journal* and constitute the core instructional materials for continuing legal education programs under The Sedona Conference Institute (TSCI banner, various International Programmes on global legal issues, and webinars on a variety of topics.

The Sedona Working Group commentaries are the product of a rigorous, open, peer-review process, described in the Preface for each one. With this volume of *The Journal*, we are initiating a more traditional double-blind peer review process for articles submitted by individual authors or small groups writing independently of the Working Group review-and-comment process. This provides readers with two distinct types of articles.

In Volume 26, Number 1, of The Journal, we offer two nonpartisan consensus commentaries from The Sedona Conference Working Group on Trade Secrets (WG12) as well as a nonpartisan consensus commentary from The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6). Sedona Canada (WG7) contributed a useful primer on Artificial Intelligence (AI) and the Law, WG6 offered Principles for International Arbitration, and we include independently authored articles on cyberattack class actions, AI in the courts, and AI in healthcare. Closing out Volume 26, Number 1, is the fourth edition of The Sedona Conference Cooperation Proclamation: Resources for the Judiciary.

I hope you find the commentaries, primer, principles, articles, and resources 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.

Kenneth J. Withers
Executive Director
The Sedona Conference
August 2025

The Sedona Conference gratefully acknowledges the contributions of its Working Group Series annual sponsors (www.thesedonaconference.org/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 Staff

Publisher
Kenneth J. Withers

Staff Editor
Craig Morgan

Editorial Consultant
Dave Lumia

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., 3M, Avondale, PA

The Hon. Mitchell D. Dembin (ret.), San Diego, CA

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., Ronald J. Hedges LLC, Hackensack, NJ

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

The Hon. Kristen L. Mix (ret.), JAG, Denver, CO

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

The Hon. Kathleen McDonald O'Malley (ret.), Sullivan & Cromwell 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.), Boies Schiller Flexner LLP, New York, NY

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

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

NAVIGATING AI IN THE JUDICIARY: NEW GUIDELINES FOR JUDGES AND THEIR CHAMBERS

Hon. Herbert B. Dixon, Jr., Hon. Allison H. Goddard, Prof. Maura R. Grossman, Hon. Xavier Rodriguez, Hon. Scott U. Schlegel, and Hon. Samuel A. Thumma

Five judges and a lawyer/computer science professor walked into a bar . . . well, not exactly. But they did collaborate as members of the Working Group on AI and the Courts as part of the ABA's Task Force on Law and Artificial Intelligence to develop the following guidelines for responsible use of AI by judicial officers. The guidelines reflect the consensus view of these Working Group members only, and not the views of the ABA, its Law and AI Task Force, The Sedona Conference, or any other organizations with which the authors may be affiliated.

The authors include:

- Dr. Maura R. Grossman, a Research Professor in the Cheriton School of Computer Science at the University of Waterloo and an Adjunct Professor at Osgoode Hall Law School of York University, who serves as a special master in both U.S. state and federal court;
- Hon. Herbert B. Dixon, Jr., Senior Judge of the Superior Court of the District of Columbia;
- Hon. Allison H. Goddard, U.S. Magistrate Judge of the U.S. District Court for the Southern District of California;
- Hon. Xavier Rodriguez, U.S. District Judge of the U.S. District Court for the Western District of Texas;

- Hon. Scott U. Schlegel, Judge of the Louisiana Fifth Circuit Court of Appeal; and
- Hon. Samuel A. Thumma, Judge of the Arizona Court of Appeal, District One.

We hope you will find these guidelines useful in your work as judges. They provide a framework for how you can use AI and Generative AI responsibly as judicial officers.

This publication may be cited as follows:

> Hon. Herbert B. Dixon Jr. et al., *Navigating AI in the Judiciary: New Guidelines for Judges and Their Chambers*, 26 SEDONA CONF. J. 1 (2025).

Guidelines for U.S. Judicial Officers Regarding the Responsible Use of Artificial Intelligence

These Guidelines are intended to provide general, non-technical advice about the use of artificial intelligence (AI) and generative artificial intelligence (GenAI) by judicial officers and those with whom they work in state and federal courts in the United States. As used here, AI describes computer systems that perform tasks normally requiring human intelligence, often using machine-learning techniques for classification or prediction. GenAI is a subset of AI that, in response to a prompt (*i.e.*, query), generates new content, which can include text, images, sound, or video. While the primary impetus and focus of these Guidelines is GenAI, many of the use cases that are described below may involve either AI or GenAI, or both. These Guidelines are neither intended to be exhaustive nor the final word on this subject.

I. FUNDAMENTAL PRINCIPLES

An independent, competent, impartial, and ethical judiciary is indispensable to justice in our society. This foundational principle recognizes that judicial authority is vested solely in judicial officers, not in AI systems. While technological advances offer new tools to assist the judiciary, judicial officers must remain faithful to their core obligations of maintaining professional competence, upholding the rule of law, promoting justice, and adhering to applicable Canons of Judicial Conduct.

In this rapidly evolving landscape, judicial officers and those with whom they work must ensure that any use of AI strengthens rather than compromises the independence, integrity, and impartiality of the judiciary. Judicial officers must maintain impartiality and an open mind to ensure public confidence in the justice system. The use of AI or GenAI tools must enhance, not diminish, this essential obligation.

Although AI and GenAI can serve as valuable aids in performing certain judicial functions, judges remain solely responsible for their decisions and must maintain proficiency in understanding and appropriately using these tools. This includes recognizing that when judicial officers obtain information, analysis, or advice from AI or GenAI tools, they risk relying on extrajudicial information and influences that the parties have not had an opportunity to address or rebut.

The promise of GenAI to increase productivity and advance the administration of justice must be balanced against these core principles. An overreliance on AI or GenAI undermines the essential human judgment that lies at the heart of judicial decision-making. As technology continues to advance, judicial officers must remain vigilant in ensuring that AI serves as a tool to enhance, not replace, their fundamental judicial responsibilities.

Judicial officers and those with whom they work should be aware that GenAI tools do not generate responses like traditional search engines. GenAI tools generate content using complex algorithms, based on the prompt they receive and the data on which the GenAI tool was trained. The response may not be the most correct or accurate answer. Further, GenAI tools do not engage in the traditional reasoning process used by judicial officers. And, GenAI does not exercise judgment or discretion, which are two core components of judicial decision-making. Users of GenAI tools should be cognizant of such limitations.

Users must exercise vigilance to avoid becoming "anchored" to the AI's response, sometimes called "automation bias," where humans trust AI responses as correct without validating their results. Similarly, users of AI need to account for confirmation bias, where a human accepts the AI results because they appear to be consistent with the beliefs and opinions the user already has. Users also need to be aware that, under local rules, they

may be obligated to disclose the use of AI or GenAI tools, consistent with their obligation to avoid ex parte communication.

Ultimately, judicial officers are responsible for any orders, opinions, or other materials which are produced in their name. Accordingly, any such work product must always be verified for accuracy when AI or GenAI is used.

II. JUDICIAL OFFICERS SHOULD REMAIN COGNIZANT OF THE CAPABILITIES AND LIMITATIONS OF AI AND GENAI

GenAI tools may use prompts and information provided to them to further train their model, and their developers may sell or otherwise disclose information to third parties. Accordingly, confidential or personally identifiable information (PII), health data, or other privileged or confidential information should not be used in any prompts or queries unless the user is reasonably confident that the GenAI tool being employed ensures that information will be treated in a privileged or confidential manner. For all GenAI tools, users should pay attention to the tools' settings, considering whether there may be good reason to retain, or to disable or delete, the prompt history after each session.

Particularly when used as an aid to determine pretrial release decisions, consequences following a criminal conviction, and other significant events, how the AI or GenAI tool has been trained and tested for validity, reliability, and potential bias is critically important. Users of AI or GenAI tools for these foregoing purposes should exercise great caution.

Other limitations or concerns include:

- The quality of a GenAI response will often depend on the quality of the prompt provided. Even responses to the same prompt can vary on different occasions.
- GenAI tools may be trained on information gathered from the Internet generally, or

proprietary databases, and are not always trained on non-copyrighted or authoritative legal sources.

- The terms of service for any GenAI tool used should always be reviewed for confidentiality, privacy, and security considerations.

GenAI tools may provide incorrect or misleading information (commonly referred to as "hallucinations"). Accordingly, the accuracy of any responses must always be verified by a human.

III. POTENTIAL JUDICIAL USES FOR AI OR GENAI

Subject to the considerations set forth above:

- AI and GenAI tools may be used to conduct legal research, provided that the tool was trained on a comprehensive collection of reputable legal authorities and the user bears in mind that GenAI tools can make errors;
- GenAI tools may be used to assist in drafting routine administrative orders;
- GenAI tools may be used to search and summarize depositions, exhibits, briefs, motions, and pleadings;
- GenAI tools may be used to create timelines of relevant events;
- AI and GenAI tools may be used for editing, proofreading, or checking spelling and grammar in draft opinions;
- GenAI tools may be used to assist in determining whether filings submitted by the parties have misstated the law or omitted relevant legal authority;

- GenAI tools may be used to generate standard court notices and communications;
- AI and GenAI tools may be used for court scheduling and calendar management;
- AI and GenAI tools may be used for time and workload studies;
- GenAI tools may be used to create unofficial/preliminary, real-time transcriptions;
- GenAI tools may be used for unofficial/preliminary translation of foreign-language documents;
- AI tools may be used to analyze court operational data, routine administrative workflows, and to identify efficiency improvements;
- AI tools may be used for document organization and management;
- AI and Gen AI tools may be used to enhance court accessibility services, including assisting self-represented litigants.

IV. IMPLEMENTATION

These Guidelines should be reviewed and updated regularly to reflect technological advances, emerging best practices in AI and GenAI usage within the judiciary, and improvements in AI and GenAI validity and reliability. As of February 2025, no known GenAI tools have fully resolved the hallucination problem, *i.e.*, the tendency to generate plausible-sounding but false or inaccurate information. While some tools perform better than others, human verification of all AI and GenAI outputs remains essential for all judicial use cases.

COMMENTARY, PRINCIPLES, AND BEST PRACTICES FOR ADDRESSING DATA RISKS ASSOCIATED WITH DAWN RAIDS IN CROSS-BORDER INVESTIGATIONS

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

Author

The Sedona Conference

Editor-in-Chief

John E. Davis

Contributing Editors

Lori Baker
Paul Brabant
Walter Delacruz
W. Warren Hamel
Ronald J. Hedges
Wayne Matus
Mariano Peruzzotti
David Shonka

Steering Committee Liaison

Leeanne Mancari

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, Principles, and Best Practices for Addressing Data Risks Associated with Dawn Raids in Cross-Border Investigations*, 26 SEDONA CONF. J. 9 (2025).

PREFACE

Welcome to the May 2025 final version of The Sedona Conference's *Commentary, Principles, and Best Practices for Addressing Data Risks Associated with Dawn Raids in Cross-Border Investigations* ("*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 John Davis for his leadership and commitment to the project. We also thank Contributing Editors Lori Baker, Paul Brabant, Walter Delacruz, Warren Hamel, Ron Hedges, Wayne Matus, Bill Marsillo, Mariano Peruzzotti, and David Shonka for their efforts, and Leeanne Mancari for her guidance and input as Steering Committee liaison to the drafting team.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG6 who reviewed, commented on, and proposed edits to early drafts of the *Commentary* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG6 meetings where drafts of this *Commentary* were the subject of the dialogue. The publication was

also subject to a period of public comment. On behalf of The Sedona Conference, I thank all of them for their contributions.

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, trade secrets, and artificial intelligence. 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.

Kenneth J. Withers
Executive Director
The Sedona Conference
August 2025

TABLE OF CONTENTS

PREAMBLE

This *Commentary, Principles, and Best Practices for Addressing Data Risks Associated with Dawn Raids in Cross-Border Investigations* ("*Commentary*") presents and discusses principles and best practices to manage data risks associated with dawn raids in criminal and civil/administrative enforcement investigations that may involve multiple jurisdictions. The *Commentary* seeks to address the unique impacts that dawn raids have on organizations' abilities to comply with data privacy and data protection requirements in cross-border matters.

Part I introduces the issues and describes the scope of the *Commentary*. Part II provides information about the prevalence and risks of dawn raids. Part III sets out eight principles for approaching and managing data risk in dawn raids and is itself divided into two sections. The first section discusses best practices of agencies with respect to achieving their goals while respecting the information rights of those affected by such raids and minimizing the collateral impact of the investigation. The second section considers best practices for organizations to follow when their information is affected by a dawn raid, whether as the subject of the raid or as a third party. Finally, an appendix provides an "Organization Data Checklist in Preparation for Dawn Raids."

I. INTRODUCTION

Government authorities, regulators, and law enforcement agencies are commonly granted extensive powers and resources to support investigations. One of the more distinctive and dramatic powers is to conduct a "dawn raid," whereby authorities—often based on judicial authorization, but sometimes based on administrative process—may, without prior notice, physically or "virtually" enter premises to search for and copy or seize information called for in the investigation.[1] Authorities view such on-site searches, and their surprise nature in particular, as critical to investigating potential misconduct in areas where concealment is expected and the specter of destruction of evidence is ever-present.[2] These raids are increasingly common in both criminal and civil/administrative investigations and may be coordinated among agencies across jurisdictions. They are at once intrusive, disruptive, and potentially threatening to the privacy and confidentiality of an organization's and a third party's seized information. The increased global use of raids coincides with continuing expansion and globalization of data flows and simultaneous surge in data privacy regulations,

1. Consistent with practice across varying jurisdictions, this *Commentary* interchangeably uses the terms dawn raid, raid, search warrant execution, and search and inspection in referencing dawn raids. Similarly, we here use the terms authorities, government authorities, regulators, and agencies interchangeably, unless otherwise indicated.

2. *See* Case T-439/07, Coats Holdings Ltd. v. European Comm'n (June 27, 2012) ("[I]t is normal for the activities that imply those practices and anti-competitive agreements to take place clandestinely, and for meetings to be held in secret, most frequently in a non-member country, and for the associated documentation to be reduced to a minimum."), cited in INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL ("INDECOPI"), DAWN RAID GUIDELINES, at 7 n.10 (2020), *available at* https://cdn.www.gob.pe/uploads/document/file/2131121/Dawn%20Raids%20Guidelines.pdf.

multiplying the resulting risks and complications. Those risks and uncertainties are compounded by the increasing prevalence of remote working practices.

What makes a dawn raid different from other types of investigative demands? The highly complex nature of multi-jurisdictional investigations causes organizations great uncertainty in preparing for and dealing with dawn raids. Dawn raids are distinct in form and effect from investigative tools that seek information on notice (such as subpoenas, civil investigative demands, requests for information, or self-executing warrants). In concept, a government authority would resort to a dawn raid when it has decided that the notice-based investigative process is insufficient to obtain information believed necessary to carry out an investigation. This decision may rest on any number of factors: e.g., the government may suspect that the organization will not fully comply with a subpoena on notice; the government may conclude that a search will be the best way to get a complete picture of the organization's activities; the evidence may be transient, mobile or threatened with destruction; and/or the agency may wish to emphasize the importance of the inquiry.

Conducting the search without notice provides the raided organization with little control over the scope, review, and use of its seized information. Raids provide fewer opportunities to perform risk assessments tailored to the inquiry, to negotiate with the investigator, and to assert legal challenges prior to disclosure of sensitive information. Organizations are further limited in their ability to control the subsequent use and transfer of protected information seized in the raid. They also are limited in the legal and practical means of mitigating a range of accompanying data risks, including loss of control, confidentiality, privacy, and privilege. As a practical matter, once the raid has commenced, some effects may be irreversible. Thus, investigating and understanding the risk, business impact, and response

options to a dawn raid differs from responding to other types of investigative demands.

Scope: This *Commentary* addresses cross-border, data privacy, data protection, and data security implications of dawn raids in criminal and civil and/or administrative enforcement contexts. Dawn raids are perhaps most notably associated with European enforcement investigations but also are widely used in other jurisdictions, including countries in the Americas and Asia. Accordingly, the topics discussed in the *Commentary* are not intended to be jurisdiction-specific. Rather, they identify and address principles and best practices applicable in a variety of locations.

This *Commentary* primarily focuses on dawn raids occurring in the context of actual or potential criminal proceedings, although in some jurisdictions authorities may also use dawn raids to conduct civil and administrative investigations.[3] Nonetheless, the practices and risks share much in common, and many of the topics discussed in this *Commentary* may be informative to those who are concerned with dawn raids in civil investigations in those jurisdictions where they are allowed. This *Commentary* complements The Sedona Conference's *International*

3. For example, the European Commission ("EC") may on its own decision or based on judicial authorization where required (e.g., where the assistance of police or an enforcement authority is necessary), conduct a dawn raid in EU member-states to follow up on prior information-gathering activities or to resolve incorrect or misleading responses to prior questioning. Council Regulation (EC) No. 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, Art. 20(2), https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32003R0001 [hereinafter EU Competition Regulation 1/2003]. National competition authorities in other jurisdictions, such as the UK's Information Commissioner's Office ("ICO") generally have similar powers.

Investigations Principles,[4] which addresses cross-border transfers of data in the context of civil governmental and internal investigations on notice, but pointedly does not delve deeply into dawn raids.

II. BACKGROUND: THE FREQUENCY AND RISKS OF DAWN RAIDS

A. *Dawn Raids: Growing Use on a Global Scale*

The use of dawn raids as an official investigative tool appears to be growing. Agency and public reports indicate that criminal, competition, tax, and enforcement authorities worldwide have increased their use of dawn raids instead of or in addition to using cooperative methods to locate and seize evidence of wrongdoing. There was a brief decline as a result of restrictions relating to the COVID-19 pandemic, but the frequency of raids returned to its prior trajectory once health and safety protocols allowed.[5] Changes in the authorizing laws have also encouraged this increase.[6]

---

4. The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices*, 19 SEDONA CONF. J. 557 (2018).

5. *E.g.*, Emilio De Geiori, *Antitrust in focus - April 2022*," JDSUPRA (May 4, 2022), https://www.jdsupra.com/legalnews/antitrust-in-focus-april-2022-4697260/.

6. For example, European competition authorities received more uniform and sometimes broader inspection powers with the 2018 enactment of the ECN Plus Directive. Directive of the European Parliament and of the council to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, 2017/0063 (COD), Art. 6 (Nov. 21, 2018) ("ECN Plus Directive"), http://data.consilium.europa.eu/doc/document/PE-42-2018-INIT/en/pdf, discussed in Maciej Marek, *Focus on antitrust dawn raids in Europe*, DENTONS (Sep. 19, 2019), *available at* https://web.archive.org/web/20190

B. Risks Relating to Dawn Raids

Organizations face substantial legal and business risks in connection with dawn raids. Third parties whose information is held by a raided organization share many of these risks. Documents and other materials seized during a raid may be used not only as evidence in enforcement actions by the agencies conducing or sponsoring the raid, but under certain circumstances may also be made available to other authorities and sometimes private litigants in related and unrelated matters. The very occurrence of a raid of an organization's offices may also lead to inquiries by authorities in other jurisdictions, who may seek access to the seized materials. A dawn raid also poses myriad collateral risks to the organization's operations, including the loss of necessary operating equipment and records, adverse publicity, conflicts with business partners and competitors, and the resulting financial implications. As discussed below, once the raid has been conducted, the seized information is out of the organization's control and often may not be easily retrieved, which highlights the need to have strong controls on the conduct of the raid before, during, and after the raid.

1. Investigative and Evidentiary Risk

The most immediate and critical risk of a dawn raid is an organization's involvement in a criminal investigation. An organization must act immediately, generally with legal counsel, to assess and respond to such risk. Lacking prior notice of a raid, organizations have far less ability to understand areas of inquiry, strategize a response, and attempt to influence the governmental actor regarding the scope, timing, method, and uses

---

920200435/https://www.jdsupra.com/legalnews/focus-on-antitrust-dawn-raids-in-europe-77155/.

of information obtained in the raid. This includes a more limited ability to bring legal challenges to seizures. (See Principle 1.)

Dawn raids also pose risks with respect to the use of the copied records as evidence in future enforcement actions and even potentially in civil litigation. Such records are, first and foremost, evidence the government can use in an ongoing or future complaint against, or prosecution of, the organization, its employees, and its business partners. That the agency obtains the documents in bulk, typically before review by the organization's lawyers, may undermine the organization's ability to identify the government's priorities and effectively speak with employees about conduct in scope. Even if the material ultimately does not support the government's suspicions, the records may alert the agency to other related or unrelated conduct, which it may choose to share with other criminal or civil enforcement agencies in certain circumstances.

The raid immediately imposes on the organization evidentiary responsibilities as well. To the extent that it did not before, the organization now knows it is involved in an investigation, generally triggering an obligation to take reasonable steps to preserve relevant evidence. This preservation obligation covers not only recorded information seized in the raid but may also include related information left behind and in other locations. It may also cover information under the organization's control but maintained by third parties. Further, the preservation obligation may extend beyond the investigation, in contemplation of related civil and criminal actions in different jurisdictions. Among other actions, the organization generally should consider a deconfliction process, instruct employees to preserve relevant information, and change its document management practices and rules to ensure the data is kept at an IT level. The

failure to implement such a "legal hold" can be significant.[7] Spoliation and obstruction concerns have breathed new life into many an investigation that was floundering on the merits.

A dawn raid may open a Pandora's Box of associated dangers. Documents seized in a raid pose elevated risks of disclosure of privileged information, as the organization may not always be able to prescreen the documents, and impromptu screens may be less thorough. A raid in any jurisdiction may sweep up privileged communications in sometimes chaotic circumstances, increasing the chances for disruption, disclosure, and waiver, even where attorneys of the organization are present and seek to quarantine privileged information. Effective screening may be frustrated by any number of factors, including the volume of data, storage medium inaccessibility, incomplete knowledge, and ineffective search terms. Remote working practices, including those affording counsel only "virtual" opportunities to aid in identifying privileged information, can make privilege protection even more difficult. Moreover, the location of the raid may be determinative, as "[p]rotections afforded to documents and information related to a party's communications with counsel and attorney work-product protections vary by jurisdiction."[8] Outside of the U.S., for example, communications between in-house counsel and employees of the organization are often *not* considered privileged.[9] Authorities in some

7. *E.g.*, The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341, 354, 359–61 (2019).

8. The Sedona Conference, *Commentary on Cross-Border Privilege Issues*, 23 SEDONA CONF. J. 475, 507 (2022) [hereinafter *Sedona Cross-Border Privilege Commentary*].

9. *Id*. at 505.

jurisdictions may also demand the waiver of privilege to secure cooperation credit.[10]

Further, "[o]nce information is produced in one jurisdiction, there is a greater likelihood that it will be discoverable in other jurisdictions."[11] Documents seized in connection with an enforcement action may be targeted in follow-on litigation, by way of civil process seeking copies of records "produced" in the search. While there is a strong presumption of secrecy in certain jurisdictions as to documents obtained in raids,[12] that will not prevent a private litigant that learns of the raid from demanding those documents directly from the organization. Alternatively, where a dawn raid is carried out by a civil or administrative authority, such as an EU state competition authority operating

---

10. Megan Zwiebel, *In New Guidance, SFO Indicates It Wants Companies to Waive Privilege*, ANTI-CORRUPTION REPORT (Oct. 16, 2019), https://www.anti-corruption.com/4103541/in-new-guidance-sfo-indicates-it-wants-companies-to-waive-privilege.thtml. *But see* The U.S. Justice Manual ("USJM") § 9-28.710 (cooperating organization is not required to waive the attorney-client privilege or attorney work product protection); SEC Enforcement Manual § 4.3 (same).

11. *Sedona Cross-Border Privilege Commentary*, *supra* note 8, at 507.

12. For example, where a U.S. dawn raid is conducted in the context of a federal grand jury investigation, the records seized in the raid should be held as confidential by the Department of Justice, either as grand jury materials subject to Rule 6(e) of the Federal Rules of Criminal Procedure, or as exempt from disclosure under the Freedom of Information Act, 5 U.S.C. § 552, based on exemptions (b)(4) and (b)(7). Thus, a civil litigant seeking access to the seized records from the government is unlikely to obtain such access, although civil process may be brought to force the organization to produce copies itself. Such secrecy is not the rule in all jurisdictions, and it may be overridden in certain circumstances. *See, e.g.*, *In re* Application of the Committee on the Judiciary, U.S. House Of Representatives, for an Order Authorizing the Release of Certain Grand Jury Materials, 414 F. Supp. 3d 129 (D.D.C. 2019) (discussing exceptions to grand jury secrecy rule, including that materials may be shared for judicial proceedings, including congressional impeachment inquiry).

under Articles 101 and 102 of the Treaty on the Functioning of the European Union, seized records may be subject to disclosure to third parties in private litigation.[13] Seizures and subsequent transfers may also implicate contract rights held by business partners or trigger an audit demand.

2. Cross-Border Risk

Raids may be conducted simultaneously or sequentially in multiple locations and jurisdictions, with authorities coordinating and sharing seized information. This compounds the risk of information disclosure contrary to legal or contractual restrictions on access, including data privacy, banking or state secrets, International Traffic in Arms Regulations restrictions, employment restrictions, medical information, privileged information, and proprietary information. Moreover, a publicized raid of an organization's offices in one jurisdiction may spark the interest of enforcement agencies in other jurisdictions in which the organization operates. For example, one investigation into a multinational construction conglomerate's alleged bribery of Brazilian government officials reportedly began with an investigation of a money laundering operation at a gas station in Brasília and subsequent raids of related entities.[14] These investigations eventually involved enforcement actions by Brazil, the U.S., and Switzerland related to the same conduct, culminating in a $3.5 billion multinational settlement. Three years later, the parent organization filed for bankruptcy protection after investigations into unrelated bribery allegations in

13. Any such disclosures to third parties would be subject to the confidentiality limitations of Art. 6 of Directive 2014/104/EU.

14. David Segal, *Petrobras Oil Scandal Leaves Brazilians Lamenting a Lost Dream*, N.Y. TIMES (Aug. 7, 2015), https://www.nytimes.com/2015/08/09/business/international/effects-of-petrobras-scandal-leave-brazilians-lamenting-a-lost-dream.html.

Argentina, Mexico, Peru, and numerous other countries in the Caribbean and South America.[15]

Cooperation among enforcement agencies has become more regularized with the use of Multinational Legal Assistance Treaties in the U.S. and similar mechanisms in other countries. For example, Switzerland—historically reluctant to share bank and financial records sought by foreign enforcement authorities—has introduced new mechanisms to work with foreign authorities in prosecuting white collar crimes and tracking the proceeds of illicit activities.[16] Another noteworthy instance within the realm of international bribery is the collaboration between the U.S. and enforcement agencies across Europe, South America, and Asia to enter into multiple Foreign Corrupt Practices Act resolutions involving multinational corporations during 2019. A raid conducted under such multilateral arrangements would undoubtedly involve the cross-border exchange of information.

3. Business Implications

Dawn raids may impact an organization's ability to carry on with its daily operations. There may be a police or inspector

15. Press Release, U.S. Dept. of Justice, Odebrecht and Braskem Plead Guilty and Agree to Pay at Least $3.5 Billion in Global Penalties to Resolve Largest Foreign Bribery Case in History (Dec. 21, 2016), https://www.justice.gov/opa/pr/odebrecht-and-braskem-plead-guilty-and-agree-pay-least-35-billion-global-penalties-resolve; *Brazil's Odebrecht files for bankruptcy protection after years of graft probes*, REUTERS (June 17, 2019), https://www.reuters.com/article/us-odebrecht-bankruptcy/brazils-odebrecht-files-for-bankruptcy-protection-after-years-of-graft-probes-idUSKCN1TI2QM.

16. Federal Act on International Mutual Assistance in Criminal Matters § 351.1, https://www.admin.ch/opc/en/classified-compilation/19810037/201903010000/351.1.pdf; *see also* Press Release, U.S. Dept. of Justice, United States and Switzerland Issue Joint Statement Regarding Tax Evasion Investigations, https://www.justice.gov/opa/pr/united-states-and-switzerland-issue-joint-statement-regarding-tax-evasion-investigations.

present onsite during the raid, bringing customer-facing and back-office business to a halt. Even if the raid can be contained in an inconspicuous area, the police or inspector will be occupying a physical space, such as a conference or IT room (or two or three), or server space, that will be unavailable for organization use.

The search team will be occupying and interacting with the office and each search site, as well as targeted systems, including seizing and copying files and equipment that employees depend on to complete day-to-day tasks. In the process, certain system accessibility might be limited, and passwords could potentially be deactivated. If the raid cannot be completed in one day, inspectors may seal premises and commandeer portions of systems pending completion. Inspectors may request to interview certain employees, pulling those individuals away from their desks for hours. Beyond the loss of productivity, an employee being interviewed creates a risk of uncontrolled disclosure of information, which may pose a significant threat to the organization. A dawn raid is a spectacle and tends to undermine productivity even if employees are working remotely or can remain at work and access the tools necessary to do their job.

The business disruptions may continue after the raid has ended. Media coverage is common, and for high-profile raids, an organization will need to devote significant time and attention to public relations. Customers may be reticent to deal with an organization under government investigation. Competitors may potentially use the raid to bolster their legal actions against the subject of the investigation, or they may even have filed complaints to the authorities that triggered the raid in the first place. The public disclosure of a prior dawn raid can also have a significant impact on an organization's chances of participating in or winning a public tender. Public information about the execution of a dawn raid may raise concerns about the organization's integrity, compliance with regulations, ethical

standards, and the organization's adherence to legal requirements, including those related to the tendering process itself. For example, procuring entities may view the organization as a higher compliance risk and choose to exclude it from the tendering process.

III. PRINCIPLES AND BEST PRACTICES WITH RESPECT TO DAWN RAIDS

The Principles set out below are intended to guide organizations in planning for and responding to dawn raids and to promote awareness and consistency among government agencies. Principles 1-5 identify data best practices among agencies for planning and conducting dawn raids. Principles 6-8 identify best practices for organizations in preparing for and responding to data implications of dawn raids.

A. Principles and Best Practices for Authorities

This *Commentary* does not purport to minimize the importance and effectiveness of dawn raids or instruct government agencies how they should go about conducting investigations. Rather, the *Commentary* has collected best practices and principles followed by various agencies conducting raids to support their critical missions. Dawn raids present complex and evolving challenges; this *Commentary* is intended to assist authorities by considering the level of process and transparency to be provided *before* obtaining the highly sensitive data often involved in these raids, and the potential collateral data risks that raids may present to third parties and regarding activities outside the scope of the investigation.

Principle 1: Dawn raids should be conducted based on a process that provides for meaningful pre-

and/or post-raid review by an independent authority.

Comment 1(a). *Right to independent review.* A fundamental principle across jurisdictions is that agency power must be subject to enforceable independent limitations, to provide guidance and guard against overreach.[17] Perhaps the most significant of these limitations is the right to independent review by a qualified tribunal of the authorization and conduct of the raid. As stated by the European Data Protection Supervisor in its Opinion 7/2019 concerning electronic evidence in criminal matters:

[E]ffective protection of fundamental rights in the process of gathering electronic evidence cross-border requires *greater involvement of judicial authorities in the enforcing Member State.* They should be systematically involved *as early as possible* in this process, have the possibility to review compliance of orders with the Charter and have the obligation to raise grounds for refusal on that basis.[18]

---

17. Indeed, such limitations are seen as vital in upholding the perception of legitimacy of agency action. One need look no further than scandals in the U.S. relating to asserted agency overreach and failures of oversight, such as the controversy over obtaining FISA warrants. *See, e.g.*, OFFICE OF THE INSPECTOR GENERAL, U.S. DEPT. OF JUSTICE, REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (Dec. 2019) (rev.).

18. European Data Protection Supervisor ("EDPS"), EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters, Executive Summary 3 (Nov. 6, 2019), https://edps.europa.eu/sites/edp/files/publication/opinion_on_e_evidence_proposals_en.pdf (emphasis in original) [hereinafter EDPS Opinion 7/2019]. *See* The International Competition Network ("ICN") Guiding Principles for Procedural Fairness in Competition Agency Enforcement, Principle Seven ("Judicial Review/Appeals: Competition agency enforcement proceedings should include the right to seek impartial review by an independent judicial body."), *available at*

Such judicial review helps to promote the existence of clear standards in terms of scope and authorization before an authority may enter premises and seize information, and to create effective and timely means by which impacted organizations and persons can raise legal objections to the raid in its aftermath. While the trend appears to be toward increased and earlier judicial involvement, considerable variation exists among jurisdictions and agencies as to the sequence and level of access to the courts that private parties may have in connection with dawn raids.[19]

Comment 1(b). *No-warrant raids and other judicial means of enforcement.* Whether raids should proceed only upon the issuance of a warrant from an independent judicial authority varies greatly among agencies and jurisdictions and has received considerable attention in the courts.[20] The ability of agencies to decide for themselves whether a raid is appropriate and how it may be conducted raises concerns of accountability and actions that may result in the abrogation of rights before they may be asserted.[21] Some courts have interpreted the laws of their

---

https://www.internationalcompetitionnetwork.org/wp-content/uploads/2018/09/AEWG_GuidingPrinciples_ProFairness.pdf (last visited Dec. 12, 2024).

19. *See generally* European Competition Network, ECN Working Group Cooperation Issues and Due Process: Investigative Powers Report (Oct. 31, 2012) § 2.1, 3.1 (2012) [hereinafter Investigative Powers Report], https://competition-policy.ec.europa.eu/document/download/357ac0f6-92fb-41aa-b1ad-a906fcdd832d_en?filename=investigative_powers_report_en.pdf (discussing EC rights and processes).

20. *See id*. § 2.3.1 at 8–9 (listing 16 jurisdictions that permit competition authorities to make inspection decisions and 14 jurisdictions that require authorization by court warrant).

21. The EC, for example, is authorized to conduct raids of organizational premises without warrants in support of investigations. Warrants are generally required only for unannounced inspections of personal premises. Members of the EU subject to their national laws, in general, have similar powers.

jurisdictions to require judicial warrants and have therefore precluded the use of evidence seized outside of such requirements.[22] Other courts, sometimes pointing to efficiency and exigency concerns, have upheld the right of agencies to act without a warrant so long as there is a meaningful and timely post-raid recourse to an impartial tribunal in order to retrieve seized data and restrict its use, including the ability to appeal warrants or

---

So do certain non-EU jurisdictions: the UK's ICO may issue an assessment notice and conduct no-notice inspections of premises, without a warrant, to determine whether a controller or processor of personal information is complying with data protection legislation, such as the GDPR or the UK Data Protection Act of 2018. These inspections can extend to any UK private business that controls or processes personal information. The evidence subject to a privacy raid can be particularly broad, and some laws put the burden on the organization to prove compliance (e.g., the accountability principle of the GDPR and similar legislation).

22. For example, on April 26, 2018, the Belgian Court of Cassation confirmed that competition dawn raids without prior warrant issued by an independent court are unlawful, and that evidence obtained through such unlawful raids was subject to an exclusionary and "fruit of the poisonous tree" rule and must be removed from the case file. This was based on the court's holding that the Belgian Constitution is more protective than Article 8 of the European Convention on Human Rights ("ECHR"), under which a judicial warrant may not always be required. *See Dawn raids without prior judicial warrant are unlawful: Court of Cassation confirms milestone judgment of Brussels Court of Appeal*, EUBELIUS (June 15, 2018), https://www.eubelius.com/en/news/dawn-raids-without-prior-judicial-warrant-are-unlawful-court-of-cassation-confirms-milestone. And in the U.S., consistent with the Fourth Amendment to the U.S. Constitution, which protects "[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures," raids in support of criminal inquiries typically require a sufficiently supported judicial warrant, including a showing of "probable cause" a crime has been committed and "a fair probability that contraband or evidence of a crime will be found in a particular place" specified in the search warrant. U.S. CONST. amend. IV; Illinois v. Gates, 462 U.S. 213, 238, 283 (1983).

post-raid judgments on issues of law and fact.[23] In June 2024, the European Union Court of Justice Advocate General issued an advisory opinion that allowing competition authorities to conduct email searches without a warrant during dawn raids is consistent with Article 7 of the Charter of Fundamental Rights of the European Union, so long as there is a legal framework with adequate safeguards against abuse such as ex post facto judicial review.[24]

Comment 1(c). *The scope of seizure should not exceed the needs of the inspection.* Clear and particularized notice of the scope of search, justified by its legitimate and articulated purposes, should be submitted to the authorizing entity in advance of the raid and later may be shared with the subject of the raid to promote transparency. While the timing of disclosure varies, it should take place in time to permit meaningful review of the

---

23. In 2015, the ECHR held that dawn raids by the French competition authority violated both the rights of defense and the right to privacy, because there were insufficient means to judicially challenge the authorization of the raid and scope of information seized. ECHR, 5th Sect., Apr. 2, 2015, n°63629/10, n°60567/10, Vinci Construction and GTM G. . .nie civil and Services v/. France**,** cited in *Antitrust Alert: Dawn Raids by French Competition Watchdog Trampled on Fundamental Rights,* JONES DAY (Apr. 21, 2015) https://www.jonesday.com/en/insights/2015/04/antitrust-alert—dawn-raids-by-french-competition-watchdog-trampled-on-fundamental-rights.

24. Imagens Médicas Integradas et al. v. Autoridade da Concorrência, Cases C-258/23 to C-260/23 (responding to 2023 Portuguese Constitutional Court ruling that searching emails solely on the authorization of the Public Prosecutor's Office without prior judicial authorization based on Art. 21 of the EU Law on Competition, violated Portugal's Constitution), *available at* https://curia.europa.eu/juris/document/document.jsf?text=&docid=287318&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1. The opinion further stated that member-states may nevertheless impose warrant-type requirements based on national law where that would not "undermine the effectiveness of the prevention of anticompetitive practices within the European Union."

actions. The authorizing entity, consistent with law enforcement imperatives and practicalities as well as familiar privacy law principles of minimization,[25] should actively work to limit the scope of raids to avoid overreach and "fishing expeditions," which present heightened risks of impact to the data rights of raid subject and third-parties.[26] The use of other investigative tools to obtain information, such as demands for production on notice, should be considered as alternatives.[27]

Comment 1(d). *Post-raid challenges to seizures of information.* Organizations impacted by raids should be permitted meaningful and timely opportunities to bring legal challenges— including to seizures and subsequent uses of information— before impartial tribunals. This post-raid forum is critical to protecting the rights of the subject and third parties and ensuring fair and equitable conduct by authorities. Justice delayed may be justice denied, and the right to challenge must be sufficiently proximate so as not to frustrate the exercise of the right. For example, a process that limits post-review challenges of the conduct of the raid (as opposed to the determination to conduct the raid) until after the final decision on the merits of a matter has been found

25. *E.g.*, Brazilian General Data Protection Law, Art. 6; Ecuadorian Personal Data Protection Law, Art. 10.

26. In Nexans France SAS and Nexans SA v. European Commission, Case T-135/09 judgement of Nov. 14, 2012, *available at* https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2012.399.01.0016.01.ENG, for example, the EU General Court annulled parts of the inspection decision because it was imprecise in its delimitation of the products concerned, which applicants claimed permitted an overly broad examination of the entirety of the organization's business in violation of general principles of EU law against arbitrary or disproportionate intervention in the sphere of private activities.

27. *E.g.*, Int'l Competition Network, Anti-Cartel Enforcement Manual, Chapter 1, § 3.1.

to provide insufficient immediate protection of rights, although there is no clear consensus in the courts on this principle.[28]

Moreover, opportunities for challenges to vindicate threatened rights must be aligned with incentives to do so. A process that permits only third parties in possession of potentially restricted information (e.g., a cloud service provider holding customer data) the right to challenge a raid or subsequent transfers, rather than the data subject, may provide insufficient protections. This concern is elevated in cases where the party in possession of the restricted information may not have standing to assert all of the rights available to the data subject, and may be prohibited from providing notice of the raid to the owner of the information.

Comment 1(e). *Exclusionary remedies.* In appropriate circumstances, courts should be empowered to issue "exclusionary" remedies under which evidence seized in violation of rights and processes must be returned, cannot be further transferred, and must not be used by agencies or others.[29] While a full treatment

---

28. *E.g.*, Delta Pekárny AS v Czech Republic, App 97/11, ECHR 279, Oct. 2, 2014 judgment (NYR). *See* INVESTIGATIVE POWERS REPORT, *supra* note 19, § 2.7 (generally discussing rights to judicial review of inspection actions of competition authorities of the EU and European Competition Network). *But see* Deutsche Bahn AG and Others v. European Commission (Case C-583/13 P) (ECJ 2015) (rejecting a challenge to a no-warrant raid based on unavailability of judicial review until after conclusion of the investigation; finding sufficient protections for fundamental rights in the EC's obligations in making decisions, various legal limitations on EC during inspection, the need for the EC to involve national authorities when force is required, and the subject's (eventual) right to review of the inspection by the European courts), *available at* https://curia.europa.eu/juris/liste.jsf?num=C-583/13&language=EN.

29. *See Belgian Supreme Court confirms illegality of dawn raids due to the lack of a warrant*, STIBBE (June 1, 2018), https://www.lexology.com/library/detail.aspx?g=2861ba72-99e5-4f0a-93a2-afcecd79ec6b#:~:text=On%2026%20April%202018

of this issue is outside of the scope of this *Commentary*, jurisdictions including the U.S. have well-developed bodies of law regarding such exclusionary rules (and exceptions), including "fruit of the poisonous tree" provisions that provide not only that evidence improperly seized cannot be used, but also that the investigators may not use other information obtained through the use of improperly obtained evidence.[30]

Although exclusionary rules can be an effective tool to impose accountability on agencies and ensure that they follow legal requirements surrounding dawn raids, there are societal costs that may be suffered by suppressing evidence of criminality based on prosecutorial mistakes and misconduct, and it is largely a disfavored remedy. Indeed, seeking suppression in U.S. courts of evidence gathered by law enforcement outside of the U.S. and shared via intergovernmental agreement typically is an uphill battle with only very limited grounds for objection.[31]

%2C%20the%20Belgian%20Supreme%20Court,of%20the%20European%20Convention%20on%20Human%20Rights%20%28ECHR%29

(discussing 2018 decision of the Belgian Supreme Court that dawn raids in the travel sector had been conducted illegally, given that protection offered by the Belgian Constitution is wider than Article 8 of the ECHR, and requiring information unlawfully obtained to be removed from the case file).

30. In Spain, the National Court in 2015 annulled fines of €61 million imposed by the Spanish competition authority on five electricity companies and their industry association, which had been based on evidence seized in a raid with inadequately defined scope. *Antitrust Alert*, *supra* note 23.

31. *See* United States v. Getto, 729 F.3d 221, 230–31 (2d Cir. 2013) (rejecting defendant's Fourth Amendment challenge to evidence received from Israeli National Police via Multinational Legal Assistance Treaty ("MLAT") because exclusionary rule applies only to foreign evidence where there is U.S. control or direction of the foreign investigation, an intent to evade the U.S. Constitution, or where the foreign agency's actions "shock the judicial conscience"), citing United States v. Lee, 723 F.3d 134, 139, n. 3 (2d Cir. 2013) (under the "international silver platter doctrine" the Fourth Amendment and its exclusionary rule do not apply to the law enforcement activities of foreign authorities acting in their own country).

Principle 2: The dawn raid procedures that authorities follow should be in writing, readily available, and consistently applied, and should inform private parties of their rights and the processes available to them for protecting those rights.

Comment 2(a). *Transparency of subject legal rights and redressability of injury.* Legal rights are more sustainable when they are known, clear, and exist within a system permitting meaningful redress.[32] As a best practice, there should be a written and readily available statement of subjects' rights and the remedies available in connection with information seizures in a dawn raid. Such rights and remedies may include the right to review the authorizing instrument during the raid, to be present for the raid, to call counsel to be present for the raid, to have privileged and confidential information of subjects and impacted third

32. Certain authorities, including the EC and the Peruvian Competition authority (Indecopi), have issued detailed written standards and guidelines for raids which they make available publicly—although the guidance may not be considered binding in the courts. *See* Explanatory note on Commission inspections pursuant to Article 20(4) of EU Competition Regulation No 1/2003, European Commission, https://competition-policy.ec.europa.eu/antitrust-and-cartels_en; DAWN RAID GUIDELINES, INDECOPI, *available at* https://cdn.www.gob.pe/uploads/document/file/2131121/Dawn%20Raids%20Guidelines.pdf (last visited Dec. 12, 2024). *See also* AUSTRIAN FEDERAL COMPETITION AUTHORITY, GUIDANCE ON DAWN RAIDS (Oct. 2017), *available at* https://www.bwb.gv.at/fileadmin/user_upload/Englische_PDFs/Standpoints%20and%20Handbooks/Guidance_on_dawn_raids_final.pdf. *See generally* Annabel, Cédric & Jorge, *Safe-raids? Meaningful judicial review of dawn raids on business premises*," EU LAW ENFORCEMENT, https://eulawenforcement.com/?p=1495 (surveying dawn raid procedures of the Commission and 9 Member States along with their prior safeguards).

parties protected pending review, and to timely seek judicial review.[33]

The following rights are consistent with the above principle:

- To review the authorizing instrument;
- To require that the search be confined to the scope authorized in the writing, and accordingly, to be able to object to any excesses;
- Generally, to be present at the raid, and to have counsel present at the raid;
- Generally, to decline to be interviewed to avoid providing potentially self-incriminating answers; to request that counsel be present if the interview occurs; and to have counsel if involved persons are arrested or detained and questioned off-site;
- To request that privileged information (as defined in that jurisdiction) not be taken or reviewed, or if the claim of privilege is disputed, that potentially privileged information be segregated until a court determines entitlement;
- To obtain an index to, and/or copy of, the information copied/seized;
- To timely review investigative minutes to ensure accuracy, including the recording of objections raised; and
- To timely challenge the determination and conduct of the raid before an independent tribunal without

33. In Argentina, for example, these rights find support in Article 18 of the Federal Constitution (right to due process and defense), the Criminal Procedure Code and other regulations such as Resolution 535-E/2017 of the Ministry of Security.

obstructing agency action (although this may not necessarily prevent the raid from occurring).

Principle 3: Dawn raids should be conducted in a manner narrowly tailored and proportionate to the circumstances and purpose of the action, so that the data rights of impacted persons are preserved and respected.

Comment 3(a). *Raids should be proportional and tailored to legitimate purposes.* The use of dawn raids should be proportionate to the investigative need. Dawn raids in general should be used only where demands for information on notice would frustrate law enforcement purposes (as where there otherwise is a credible risk of spoliation of evidence or evasion of the demand), the inspection is appropriately and narrowly restricted to the subject matter and articulated purpose of the inspection, and the raid is conducted in a manner that preserves the information rights at issue (e.g., so that privileged information is not reviewed by inspectors outside of the privilege challenge process).

Comment 3(b). *Considerations to Promote Proportionality.* Heightened attention should be paid to ensuring that other less intrusive and less cooperative means of compelling disclosure to the agency are not available or would unacceptably undermine the investigative purpose.[34] Best practices may be promoted by asking:

---

34. Proportionality principles are generally applied in structuring and limiting data transfers in international investigation and disclosure efforts. *See generally* The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices*, 19 SEDONA CONF. J. 557, 612 (2018) (Principle 4, cmt. 4d, citing GDPR art. 5(b)–(d)) ; *see also In re* Bard IVC Filters Prods. Liability Litig., 317 F.R.D. 562 (D. Ariz. 2016) (rejecting on proportionality grounds discovery request for marginally relevant document located in EU

- Can the evidence be obtained through other (less intrusive) means?
- Would a demand for information on notice frustrate law enforcement purposes? Is there a credible risk of spoliation of evidence absent the raid?
- Is a dawn raid appropriate for the level of offense being investigated?
- Are the rights of impacted persons adequately preserved through the warrant process and/or via post-raid challenge?
- Is the examination appropriately restricted to the subject matter and articulated purpose of the inspection?
- Is collection appropriately targeted (e.g., through use of data screening, filtering, and other minimization techniques) to mitigate risks to subject and third-party rights?
- What rules will be followed by the investigative team to ensure these principles are met, and that the raid is conducted in a manner to preserve the right to review?
- How is privilege to be protected?[35]

---

where most of the relevant materials were also in the U.S.); Principle 2 cmt. (citing FED. R. CIV. P. 26(b)(1) (scope of discoverable information restricted by proportionality; listing factors in proportionality determination).

35. Many agencies maintain such internal procedures. For example, in its Regulatory Action Policy, the ICO sets out its enforcement policy under the Data Protection Act of 2018. In general, it reserves dawn raids and other of its most intrusive enforcement powers for high-impact, intentional, willful, neglectful, and repeated breaches of data protection law. Further, in order to obtain such a warrant, the ICO will need to satisfy the court of the reasons for urgent access to the premises, and that providing notice would frustrate the purpose of the inspection, e.g., that evidence would be destroyed if notice

Comment 3(c). *Special considerations should apply to attorney and law office searches.* The risks to privileged and other protected information posed by raids of law offices are especially pronounced. Typically, special procedures must be followed and specific showings made to initiate such a raid, and special processes are put in place to protect privileged information. However, the nature and consistency of such protections vary widely across jurisdictions, as does the definition of protected information and who may enforce such protections.[36]

These problems and the difficulties of adequately protecting privilege were on display in the raid conducted in September 2015 by German prosecutors of the Munich law offices of outside counsel for Volkswagen. This was in connection with a criminal investigation of emissions fraud by its subsidiary, Audi. The raid was authorized by court order but lacked

---

was provided. INFORMATION COMM'RS OFFICE, REGULATORY ACTION POLICY (2018) at 12, *available at* https://www.scribd.com/document/818313802/ICO-regulatory-action-policy; DPA Section 149(2). *See also* COMPETITION & MARKETS AUTHORITY, COMPETITION ACT 1998: CMA GUIDANCE AND RULES OF PROCEDURE FOR INVESTIGATION PROCEDURES UNDER THE COMPETITION ACT 1998 (Mar. 2014), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/288738/CMA8resp_CA98_CMA_Guidance_and_Rules_of_Procedure_SoR.pdf.

See also ICN ANTI-CARTEL ENFORCEMENT MANUAL, *supra* note 27, Ch. 1, § 3.1 (certain agencies will conduct a search only if other investigative tools would not be effective; setting out "needs" test asking "whether there are other reasonable and less intrusive means to obtain the information sought").

36. *See generally* USJM, *supra* note 10, § 9-13.420 (Searches of Premises of Subject Attorneys), https://www.justice.gov/jm/jm-9-13000-obtaining-evidence. *See also* Klitzman, Klitzman, and Gallagher v. Krut, 744 F.2d 955 (3d Cir. 1984) (requiring courts to "scrutinize carefully the particularity and breadth of the warrant authorizing the search, the nature and scope of the search, and any resulting seizure"; finding warrants overbroad because they permitted seizure "without regard to whether the materials had any connection to particular alleged crimes or to [subject matter] in general").

sufficient safeguards to recognize and preserve privilege, and post-raid efforts to protect the privilege were largely unsuccessful. In July 2018, Germany's high court rejected a challenge to the raid brought by Volkswagen and the law firm. The court held that the raid did not impermissibly permit the review of privileged documents because, under German law, the seized communications were not privileged—the law firm was engaged only by the parent organization, not the subsidiary that was the target of the Munich prosecutors. Further, the Munich offices of the law firm were found to have no constitutional right to bring a challenge because the firm was headquartered in the U.S. The court stated that a contrary ruling invited important evidence being "purposefully stored with lawyers or only selectively published."[37]

---

37. *See* Jack Ewing and Bill Vlasic, *German Authorities Raid U.S. Law Firm Leading Volkswagen's Emissions Inquiry*, The New York Times (Mar. 16, 2017) *available at* https://www.nytimes.com/2017/03/16/business/volkswagen-diesel-emissions-investigation-germany.html; Ana Reyes and Matthew Heins, *Jones Day Case Highlights Questions Of Atty Privilege Abroad*, LAW360 (July 27, 2018), https://www.wc.com/Resources/128507/Ana-Reyes-and-Matthew-Heins-Co-Author-Questions-of-Attorney-Privilege-Abroad. Other courts, albeit a minority, have expressed suspicion of dawn raids executed on attorney offices or law firms, because of the risk of violating attorney-client privilege and attorney work-product protections. *See* Cohen v. United States, No. 1:18-mj-03161, 2018 WL 1772209 (S.D.N.Y April 13, 2018), ECF No. 30 (April 27, 2018) (barring government team from accessing materials seized in search warrant executed at offices of attorney Michael Cohen and appointing a special master to review seized materials for relevance and privilege, including an opportunity for defense counsel to challenge the special master's determinations, prior to production of materials to government prosecutors); *see also In re* Search Warrant Dated June 13, 2019, 942 F.3d 159 (4th Cir. 2019) (in granting preliminary injunction against government, halting review of records seized in search warrant of a law firm, court observes: "Federal agents and prosecutors rummaging through law firm materials that are protected by attorney-client privilege and the work-product doctrine is at odds with the appearance of justice."). *Cf.* Harbor Healthcare Systems, L.P. v. United

Comment 3(d). *Organizational planning issues.* This principle implies corresponding best practices for organizations that have information seized in dawn raids. Relevant issues for the private parties to address include:

- **The location of data can be determinative (including to what extent it is accessible across borders).** Local law of privilege, including whether corporate group members are protected under representation, varies tremendously and may provide traps for organizations that are not mindful of what has been seized. Organizations in their dawn raid planning should identify where sensitive documents are held and from where they are accessible, as well as what remedial measures may mitigate risks. (See Principle 7.)
- **The extent to which privileged communications can be protected in law offices headquartered outside of the location of the raid**. Dawn raid planning should include an assessment of attorney-created documentation and attorney-client communications—what is privileged, and who is a client, under local law and regional law (which may be superseding). Documents prepared by in-house lawyers, for example, are likely not privileged in a European Commission ("EC") investigation even if they are considered privileged under the member-state laws

States, 5 F.4th 593 (5th Cir. 2021) (per curiam) (criticizing prosecutors' refusal to destroy or return to the organization's privileged information obtained in raid of corporate offices, in case later use desired). *But see In re* Sealed Search Warrant, 11 F.4th 1235 (11th Cir. 2021) (per curiam) (broadly rejecting contention that use of governmental "taint teams" to self-screen for privileged material seized from targets of criminal investigations is inappropriate; citing cases).

of many EU countries. In addition, the EC may determine that EU law applies when it seeks documents created under privilege in the U.S. and shared with non-U.S. entities, squarely setting up a conflict with U.S. privilege law. To illustrate the point, in the Volkswagen investigation, the attorney engagement letters did not support the assertion of privilege under local law, which had a far-reaching impact on the organization's ability to protect that sensitive information from disclosure.

- **The extent that exposure of privileged documents in one jurisdiction controls the privilege status of the documents in another jurisdiction**. Following the Volkswagen raid discussed above, plaintiffs in a German civil action filed a petition in U.S. courts under 28 U.S.C. § 1782 (which permits discovery in aid of foreign proceedings) to obtain the internal investigation documents held by the law firm. The court applied U.S. law to hold that an attorney-client relationship broadly existed between the law firm and Volkswagen, protecting those documents from use in the civil action.[38] However, other courts have found that documents were discoverable in a U.S. court proceeding when the documents would have been privileged under U.S. law but were not considered privileged under foreign law.[39]

---

38. *In re* financialright GmbH, No. 17-mc-105, 2017 WL 2879696 (S.D.N.Y. June 22, 2017), citing *In re* Parmalat Securities Litigation, No. 04-MD-1653, 2006 WL 3592936, at *5-6 (S.D.N.Y. Dec. 1, 2006).

39. Wultz v. Bank of China Ltd., 979 F. Supp. 2d 479, 492–93, 495–96 (S.D.N.Y. 2013). *See also* United States v. Getto, 729 F.3d 221, 227–28 (2d Cir. 2013) (MLATs permit U.S. authorities to obtain and rely upon data seized by

Principle 4: Dawn raids should be conducted with due respect for the data privacy, protection, and localization laws of sovereigns whose citizens and residents are affected by the raids, as well as the rights and interests of persons who are subject to such laws.

Comment 4(a). *Dawn raids may lead to cross-border conflicts of law.* Authorities in dawn raids commonly seize electronically stored information ("ESI") from the raided premises.[40] Moreover, authorities increasingly reach for ESI that is accessible from the premises but located remotely, including ESI that is in the cloud or held by employees working remotely.[41] Potential

---

foreign authorities even where the same such seizure would have been unconstitutional if conducted in the U.S.).

40. *E.g.*, Section 27(5)(b) of the UK Competition Act 1998 (authorizing Competition & Markets Authority officers to require any relevant ESI that is accessible from the searched premises to be produced for seizure, preserved, and to prevent interference with such steps).

41. The EC has long asserted the right to access all information that is accessible to the inspected entity. *See* Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforces and to ensure the proper functioning of the internal market, Art. 6 (EC inspectors have the right to access all information accessible to the inspected entity, making no exception for location), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0001. The validity and contours of this "access principle" have not been squarely tested in a court of law. *See* Organisation for Economic Co-operation and Development (OECD), Directorate for Financial and Enterprise Affairs Competition Committee, Investigative powers in practice – Unannounced Inspections in the Digital Age and Due Process in relation to Evidence Gathering, at 2, https://one.oecd.org/document/DAF/COMP/GF/WD(2018)25/en/pdf. The EC's approach is not the only one, however. Other agencies adopt a "Location approach," where they look purely at where the digital information is stored as described in the authorizing order; to look beyond that location, the agency must obtain another order. See ICN ANTI-CARTEL ENFORCEMENT MANUAL, *supra* note 27, Chapter

conflicts with foreign data privacy and protection laws and export restrictions arise where such ESI is drawn from outside of the country. This sort of compelled cross-border transfer raises concerns of the foreign sovereign and those whose data are subject to its laws and potentially requires the organization to violate such foreign laws in enabling the transfer instruction. Yet refusing to enable the transfer places the organization at risk of being labeled obstructive, with accompanying penalties, negative inferences, and other consequences. (See Principle 6.)[42] Authorities should recognize those concerns and, when enforcement priorities allow, consider adopting policies and practices to minimize these types of conflict.

Comment 4(a)(i). *"E-Raids."* Reflecting the way that organizations conduct and document their business, the great bulk of evidence sought and acquired in dawn raids is in digital form. Such data is often stored on cloud-based systems that may be accessed remotely. Investigators conducting an "E-raid" may in place of, or in conjunction with, the raid of the physical premises, schedule a video conference and extract passwords and access to organization and employee systems and devices. The investigator may then review and/or remotely copy data (often with organization representatives permitted to monitor the process). Such attendees, systems, and devices may be in locations outside of the jurisdiction of the investigating agency.

---

on Digital Evidence Gathering § 8.4 (noting that where new sources of data outside of the jurisdiction are identified, steps may be taken to immediately arrange for preservation of such data including through the 24/7 Network, pending legal process).

42. The Sedona Conference's *Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders*, 21 SEDONA CONF. J. 393 (2020), provides an excellent discussion of conflicts-of-law risks and factors involved in cross-border data transfers.

E-raids may also reach outside of the office. There is a long-term trend toward remote work, at home or other locations outside of the organization office (including in different jurisdictions). Employees are doing business and otherwise creating records of interest with their personal devices and providers (including messaging apps like WeChat or WhatsApp, and cloud-based third-party services and repositories like Google Drive and Box). Agencies have responded by requiring employees to come into the office and bring their devices for inspection and by going to employees' residences to collect data. Home raids with collections of data from personal devices and nonorganization repositories raise significant privacy concerns.[43]

Yet further challenges can occur when the organization does not participate in the raid at all. Some have expressed concern about cybersecurity and national intelligence laws providing authorities extrajurisdictional access to data hosted by service providers without cooperation of the host country, much less the owners of the information.[44] Agencies use strategies (what

---

43. For this reason, home raids in the EU typically require a judicial warrant from a national court, although the line between work and home is becoming blurred. *See supra* n.21. Companies should prepare their employees for the possibility of such actions. In October 2021, the UK Financial Conduct Authority (FCA) issued guidance on the implications of remote work, noting: "It's important that firms are prepared and take responsibility to ensure employees understand that the FCA has powers to visit any location where work is performed, business is carried out and employees are based (including residential addresses) for any regulatory purposes. This includes supervisory and enforcement visits." *Remote or hybrid working: FCA expectations for firms*, FCA (last updated Feb. 13, 2023), https://www.fca.org.uk/firms/remote-hybrid-working-expectations.

44. European Commission, Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data (Feb. 29, 2020), at 9, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

the FBI calls "Network Investigative Techniques" or "NIT") to surreptitiously gain remote access to, and seize, electronic information. These seizures reportedly have taken place across international borders.[45] Moreover, under the "access principle,"[46] the boundaries of an electronic seizure need not necessarily be articulated in a legal order authorizing the search; the investigator may simply follow access points to their conclusion. Subjects of such investigations would be unable to influence the course of the raid by scrutinizing the authorizing instruments, raising objections in real time (or, in some cases, at all), or to advocate for special procedures to identify and secure privileged, sensitive, and protected information. Subjects who do not learn of the raids until after the seizure is complete (if at all) may further struggle to understand even what was taken, hampering their ability to investigate the circumstances, take remedial action, or to mount a defense.[47]

These concerns also exist in the case of "remote warrants," which enable investigators in the U.S. to search media located outside of their jurisdiction. In 2016, the U.S. adopted changes to the Federal Rules of Criminal Procedure ("FRCrP") that loosened restrictions for government agents executing a remote

---

45. Jeff Welty; *Search Warrants Authorizing Law Enforcement Computer Hacking and Malware*, NORTH CAROLINA CRIMINAL LAW (Jul. 23, 2018), https://nccriminallaw.sog.unc.edu/search-warrants-authorizing-law-enforcement-computer-hacking-and-malware/.

46. *See supra* n.41.

47. Agencies including the U.S. Department of Justice ("DOJ") may seek "warrants that excuse agents from having to notify at the time of the search the person whose premises are searched." U.S. DEPT. OF JUSTICE COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION CRIMINAL DIVISION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, at 83, *available at* https://www.justice.gov/usdoj-media/criminal/media/1178781/dl?inline.

.

search warrant."[48] These changes authorize the government to search computers located outside the jurisdiction of the magistrate judge issuing the warrant. These searches—like the NIT searches described above—were developed to deal with increasingly sophisticated cybercriminals who deploy obfuscation technology to evade law enforcement. Prior to the changes, the government could only issue search warrants outside of their districts in limited circumstances, such as when a tracking device was installed within the district and moved outside of the district, or in cases of terrorism investigations.[49] The 2016 changes to FRCrP Rule 41, however, allow the government to remotely access a suspect's computer when the suspect has obscured the location by using anonymizing technology such as a proxy server or a Virtual Private Network.[50] The amended Rule 41 therefore allows the government to execute a search warrant that requires accessing a computer network outside the district where the warrant was issued.

While many of the early and more aggressive applications of these remote search warrants stemmed from investigations involving child pornography, the statute does not so limit their use. For organizations that do business around the world, this tactic increases the chances that an organization network or device could be swept up in an investigation where the organization or an employee is merely tangentially related.

48. FED. R. CRIM. P. 41(b)(2)-(5).

49. *Id.*, advisory committee's note to 2016 amendment.

50. *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches*, U.S. DEPT. OF JUSTICE (June 20, 2016), https://www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches.

Organizations should consider such risks in determining what content is permitted to pass through their servers.[51]

Comment 4(b). *Intergovernmental comity considerations.* Consistent with comity principles, authorities conducting dawn raids generally should not unilaterally access data located in a foreign jurisdiction. Instead, the investigating authority should gain the permission or enlist the assistance of the resident foreign authority through an agreed upon procedure, a bilateral/multilateral agreement, or other intergovernmental cooperation mechanism.[52] The foreign authority may then evaluate the

---

51. By contrast, self-executing warrants enable law enforcement to send a warrant to an organization instructing it to conduct a search. *See, e.g.*, United States v. Bach, 310 F.3d 1063, 1067 (8th Cir. 2002) (upholding use of search warrant faxed to internet communication company asking it to conduct the search for records, finding that the "Fourth Amendment does not explicitly require official presence during a warrant's execution," and that "[c]ivilian searches are sometimes more reasonable than searches by officers."), citing cases. For example, a self-executing search warrant reviewed by the authors of this article was signed by a magistrate judge and served on an organization and includes instructions as to how to execute the warrant in addition to the description of items to be "seized" by the "government," or in this case, the recipient. The recipient is "ordered to disclose the [requested] information to the government within 14 days of the issuance of this warrant." The self-executing warrant is not a dawn raid but functions more in the nature of a subpoena in its execution and so abides by judicial warrant requirements and generally provides the recipient far more opportunities to shape and respond to the government's demands than would a traditional raid.

52. *See* Principle 1 of The Sedona Conference's *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation* (Jan. 2017), at 9 ("in a U.S. legal proceeding, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws"), *available at* https://thesedonaconference.org/publication/International_Litigation_Principles. *Cf.* EDPS Opinion 7/2019, *supra* note 18 (noting that involvement of member state is needed to enforce data subject rights, which may differ across jurisdictions).

request and obtain the data in its jurisdiction in conformity with its own laws and process. That may include first screening such information for restricted information or providing the holder the opportunity to influence and challenge the seizure and process in advance of the requested acquisition and transfer, and appropriately remediating the data set before transfer.

This restraint is consistent with rules, laws, and guidelines of many authorities that require consideration of such deferential processes in acquiring data stored outside of the jurisdiction.[53] The U.S. Cloud Act, while outside of the scope of this *Commentary*, is a recent example of a statutory scheme that promotes deference to foreign jurisdictions when obtaining extraterritorial data.[54]

---

53. For example, the DOJ, often with the FBI or other agencies, may work with authorities outside of the U.S. via intergovernmental MLATs and other mechanisms to conduct coordinated raids at a foreign organization location. (USJM, *supra* note 10, § 9-13.500-525). When considering issues of obtaining evidence abroad, the Justice Manual requires consideration of the appropriate method to gain that country's assistance. *See id.*, § 9-13.510, Obtaining Evidence Abroad—General Considerations ("Every nation enacts laws to protect its sovereignty and can react adversely to American law enforcement efforts to gather evidence within its borders without authorization. Such efforts can constitute a violation of that nation's sovereignty or criminal law. You should contact the Office of International Affairs, Criminal Division, as soon as you become aware that you may need evidence located in another country to determine methods for securing assistance from abroad and to select an appropriate one."). *See also* Article 22(1) of EU Competition Regulation 1/2003, *supra* note 3, Art. 22(1) (competition authority from one EU member-state may carry out an inspection on behalf and for a competition authority from another member-state).

54. The Clarifying Lawful Overseas Use of Data Act (Cloud Act), 18 U.S.C.A. § 2523 (2018), in brief, authorizes warrants issued on certain U.S. electronic communications and cloud providers under the 1986 Stored Communications Act ("SCA") to reach communications stored outside of the U.S. Such warrants may be quashed if (a) the disclosure would cause the provider to violate foreign laws; (b) "based on the totality of the circumstances, the

Comment 4(c). *Procedures to promote comity.* Authorities should put in place procedures to avoid or minimize conflicts with foreign data protection requirements for seized information. For example, U.S. courts will employ comity considerations when evaluating whether foreign data protections should be enforced as an evidentiary privilege in the U.S. Similarly, U.S. courts generally recognize the attorney-client privilege when a U.S. lawyer advises a foreign organization on U.S. law, even if that privilege would not be recognized under the foreign law.[55]

---

interests of justice dictate that the legal process should be modified or quashed; and" (c) "the customer . . . is not a United States person and does not reside in the United States." A court hearing a challenge to the Cloud Act warrant will perform a comity analysis and consider "the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure" and "the interests of the qualifying foreign government in preventing any prohibited disclosure." This solution—while not directly permitting challenge by the data subject—tends to mitigate providers' fears that complying with SCA warrants for extraterritorial data would require violation of foreign law. The Cloud Act also authorizes reciprocal rights to non-U.S. jurisdictions that, in entering into a bilateral agreement with the U.S., prequalify to make requests directly to U.S. service providers for SCA information maintained in the U.S., rather than proceeding via an MLAT. *See also* discussion of proposed EC E-Evidence Directive, *E-evidence – cross-border access to electronic evidence*, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en (last visited Dec. 13, 2024).

55. *See* The Sedona Conference, *Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders*, 21 SEDONA CONF. J. 393 (2020); Wultz v. Bank of China Ltd., 979 F. Supp. 2d 479, 492–93, 495–96 (S.D.N.Y. 2013). *Cf.* Akzo Nobel Chemicals Ltd. and Akcros Chemicals Ltd. v. Commission of European Communities, (Joined Cases T-125/03 and T-253/03 (2007) (in-house counsel are not "independent" and so their communications are not privileged; legal professional privilege covers internal documents drafted solely to seek advice from external lawyers). Reportedly, the legal advice of inside counsel relied upon by the EC in finding that John Deere & Co. knowingly violated EU anticompetition law had been provided

Comment 4(d). *Considerations when intergovernmental cooperation is lacking.* It is a reality that certain countries will not always cooperate in foreign agency investigations, frustrating the efforts of law enforcement. Some objections may be principled—a country may deny a request for assistance in obtaining data to investigate something that is not illegal in the country where the data is located (e.g., criticisms of a government are likely protected activity in the U.S., although they may be a crime in other jurisdictions). Some objections, however, may be parochial or even corrupt.

When the agency seeks to go it alone on this basis, the various interests may best be weighed through a pre-raid submission, similar to a warrant, that permits a court to apply comity principles. An authority determined to engage in "self-help," in contrast, may face a stiffer burden in a post-raid challenge to the seizure, when hindsight reigns and it may be unable to take affirmative steps to help justify its actions. The U.S. Supreme Court in *Société Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa*, set forth the following five factors to consider in determining whether a foreign data restriction must be complied with: (1) the importance to the litigation of the documents or other information requested; (2) the degree of specificity of the request; (3) whether the information originated in the U.S.; (4) the availability of alternative means of securing the information; and (5) the extent to which noncompliance with the request would undermine important interests of the U.S., or

---

by counsel to organization management in the U.S. and Germany in a memo that was seized in a dawn raid on European offices. Case L-35/38, John Deere & Co. v. N.V. Cofabel, 14 December 1984 O.J.L. 35, 2 C.M.L.R. 554. I, at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1985:035:FULL:EN:PDF at 61, discussed in *European Court of Justice Finds In-House Legal Advice Not Protected by Legal Professional Privilege*, SIMPSON THACHER (Sept. 17, 2010), https://www.stblaw.com/docs/default-source/cold-fusion-existing-content/publications/pub1061.pdf.

compliance with the request would undermine the important interests of the state where the information is located.[56] Some courts have also considered the negative impact of the producing party being out of compliance with the foreign law.[57]

> **Principle 5:** There should be meaningful restrictions on the immediate access by authorities to privileged and protected information during a raid, and on the review, use, disclosure, and ultimate disposition of such information.

Comment 5(a). *Special procedures for protected information.* As is feasible, seizures should be restricted to information within the scope of the authorizing instrument, which should be narrowly tailored (See Principle 3). Moreover, investigators should not seize or review information where there are reasonable grounds to believe the material is unreviewable on the ground of privilege. For ESI in particular, it may be easy and tempting for authorities to scoop up information that is out of scope or protected, then sort and analyze later.[58] In contrast to the use of

---

56. Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa, 482 U.S. 522, 539–40, 544 (1987) (quoting RESTATEMENT OF FOREIGN RELATIONS LAW (REVISED) (1986)).

57. Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1475 (9th Cir. 1992) (citing *Aérospatiale*, 482 U.S. at 543–44 n.28).

58. UK ATT'Y GEN.'S OFFICE, ATT'Y GEN.'S GUIDELINES ON DISCLOSURE - FOR INVESTIGATORS, PROSECUTORS AND DEFENCE PRACTITIONERS, at 24-25 (Dec. 2013), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/262994/AG_Disclosure_Guidelines_-_December_2013.pdf (authorizing retention of irrelevant information "inextricably linked" to relevant information, and cautioning investigators not to be overly quick in disregarding such irrelevant information due to potential for case requirements later). Such overcollection and retention may cause considerable downstream problems in controlling information and

investigative tools based upon notice, raided companies are in a poor position to clarify legitimate scope, tailor the response, or identify and segregate for special treatment information that should not first be reviewed by the authority.

Authorities should develop special procedures to protect privileged or otherwise protected information in dawn raids, to isolate such information without betraying the privilege,[59] and to provide organizations the ability to assist in its identification and sequestration before exposure.[60] As discussed below,

---

investigation risk and may be the focus of time-consuming efforts to retrieve out-of-scope data.

59. For example, EC officials generally are prohibited from reviewing or seizing documents that are, or are asserted to be, protected by a legal privilege. *See* INVESTIGATIVE POWERS REPORT, *supra* note 19, § 2.5 (discussing variations of process for protecting legal professional privilege during raids); OECD, Directorate for Financial and Enterprise Affairs Competition Committee, Summary of discussion of the roundtable on the treatment of legally privileged information in competition proceedings [hereinafter OECD LPP Report] (discussing "sealed envelope procedure" where investigator may physically seize or copy documents and family members for later determination of privilege by Directorate-General for Competition's Hearing Officer, which acts as an independent arbiter regarding procedural disputes between targets/third parties and EC investigators), https://one.oecd.org/document/DAF/COMP/GF/WD(2018)25/en/pdf. *See generally* Wouter P. J. Wils, *Legal Professional Privilege in EU Antitrust Enforcement: Law, Policy & Procedure*, WORLD COMPETITION L. & ECON. REV., Vol. 42, No. 1 (March 2019), at 21–42. In addition, the DOJ has developed guidelines for obtaining, protecting, and further transferring protected information, including information subject to foreign laws, and potentially privileged information. *See* USJM, *supra* note 10, §§ 9-13.400-.512.

60. Such guidelines of conduct are embraced by regulators as well as subjects of raids. The ICN has commented directly on such procedural transparency and inclusiveness, and the need to address confidentiality and privilege concerns arising from inspections and enforcement actions. *See* International Competition Network (ICN) Guiding Principles for Procedural Fairness in Competition Agency Enforcement ("Meaningful Engagement: Competition agencies should seek and take into account relevant information and views

authorities have developed several different practices that may be effective in a given situation.

Comment 5(b). *The use of "taint teams" to protect privilege.* One such procedure is to sequester privileged information from the investigative team before an independent determination of privilege. This may be done by isolating the documents in a neutral manner (e.g., through technology) and then either permitting counsel for the subject to first review the seized data for privilege or routing such documents to a special review team with independence from the investigative team.

Authorities may arrange for the creation of a "taint team" composed of persons working for the investigating agency who are walled off from the investigative team, or, in circumstances where a court has been engaged, a special master or independent counsel to review the seized materials for privileged documents and communications. In theory, privileged information may thus be excluded from review by the investigators, who will not be "tainted" by the information.[61]

---

from parties and third parties to inform their consideration of enforcement matters. Agencies should offer meaningful communication with parties on significant factual, legal, economic, and procedural issues at key points during enforcement . . . .") ("Confidentiality Protections: Competition agency enforcement proceedings should include a process for appropriate identification and protection of confidential business information and recognition of privileged information. The decision to disclose confidential information should include consideration of the confidentiality claims, rights of defense, rights of third parties, incentives to provide information, effects on competition, and transparency to the public."), available at https://www.internationalcompetitionnetwork.org/wp-content/uploads/2018/09/AEWG_GuidingPrinciples_ProFairness.pdf

61. The U.S. Justice Manual provides for the use of a "privilege team" "to protect the attorney-client privilege and to ensure that the investigation is not compromised by exposure to privileged material." USJM, *supra* note 10, § 9-13.420(e). The DOJ considers this an internal process that creates no rights in the event the guidelines are not followed.

Variations of such procedures are common. For example, the Netherlands Authority for Consumers and Markets, upon assertion that data to be inspected contains privileged correspondence, will take a "cursory look" at the data and either set it aside or, if not convinced that it is privileged, will route the data to an uninvolved Legal Professional Privilege officer for further review.[62]

Beyond using different personnel, additional steps may be taken to protect the rights of the data owners and subjects. The review team should consist of people who are knowledgeable about the subject matters of the investigation, are well-versed in the nuances of relevant privilege laws, and are operationally independent of the investigators. Investigators should not review any materials in scope before the taint team clears them for investigative review and analysis. Authorities should consider consulting with counsel for the data owners and subjects to better identify the subject information, consistent with counsel's obligation to protect client confidentiality. Further, counsel should receive access to the seized materials as soon as practicable and be given a meaningful opportunity to object to further use by the investigators of any document that has been released to them.

The use of taint teams composed of prosecutors and other persons who may appear to lack independence from the investigative agency, as well as the "cursory look" practice, are controversial. These practices may raise the specters of conflicts, create greater incentives to construe privilege narrowly, increase the risk of leakage of privileged and irrelevant

62. *See* The Netherlands Authority for Consumers and Markets, 2014 ACM Procedure regarding the legal professional privilege of lawyers, *available at* https://www.acm.nl/sites/default/files/old_publication/publicaties/12771_2014-acm-procedure-regarding-the-legal-professional-privilege-of-lawyers-2014-02-06.pdf.

information (either to the investigating team or for unrelated matters), and have an adverse impact on principles underpinning the privilege, such as the free flow of information between attorney and client. While generally accepted, some U.S. courts have rejected the idea that review of privilege information by other prosecutors—even if procedurally walled off—is acceptable and have required the appointment of an independent reviewer in situations where privilege risks are pronounced, such as searches of law offices.[63] At least one appellate court has found such practices to violate fundamental U.S. principles of separation of powers due to judicial functions being arrogated by the executive.[64] In other instances, courts have held that

63. *See, e.g.*, United States v. Gallego, No. 4:18-cr-01537-001-TUC-RM (BPV), 2018 WL 4257967, at *3 (D. Ariz. Sept. 6, 2018) (ordering special master be appointed instead of DOJ taint team), quoting United States v. SDI Future Health, Inc., 464 F. Supp. 2d, 1027, 1037 (D. Nev. 2006) ("federal courts have generally 'taken a skeptical view of the Government's use of 'taint teams' as an appropriate method for determining whether seized or subpoenaed records are protected by the attorney-client privilege.'").

64. This was the conclusion of the Fourth Circuit Court of Appeals in *In re* Search Warrant Issued June 13, 2019, 942 F.3d 159 (4th Cir. 2019). The Court found that the ex parte order of the special master authorizing the use of a "filter team" of federal agents, prosecutors, and forensic examiners to review a criminal defense law firm's records seized under warrant violates separation of powers and fails to effectively protect privilege. *Id.* at 182–83 ("It would be difficult for reasonable members of the public to believe that Filter Team AUSAs would disregard information in Lawyer A's emails that might be relevant to other criminal inquiries in Maryland."). The Court enjoined the taint team review and ordered the records to be provided to a special master to perform that function. *See id.* at 178 ("In sum, the Filter Protocol improperly delegated judicial functions to the Filter Team . . . which left the government's fox in charge of guarding the Law Firm's henhouse."). *See supra* n.63 (discussing case law). The Court of First Instance of the EU similarly disapproved of the EC's "cursory look" practice where there is any doubt or dispute about whether a document is protected by the legal professional

judicial approval of an intra-agency taint team should not be granted in ex parte proceedings, given the risks of irreparable harm to privilege and the adversary system implicated by law office searches.[65]

Comment 5(c). *Additional Screening Procedures and Artificial Intelligence (AI).* Additional measures may be needed to appropriately address owner and subject data property and privacy rights. Design of these measures should take into account the nature of the data and the means to isolate the sensitive information and may require a team knowledgeable about the technical solutions available to facilitate such a process.

Even where a taint team is used, authorities should consider screening mechanisms to identify potentially privileged information in a seized dataset that minimize risk to privilege. Investigators may bring in counsel for data owners and subjects to identify privileged information. Where there is disagreement as to an objection to disclosure, interested parties may be given an opportunity to have their objections considered by an impartial neutral party.[66]

---

privilege. *Akzo Nobel Chemicals Ltd. and Akcros Chemicals Ltd. v. Commission of European Communities,* (Joined Cases T-125/03 and T-253/03 (2007).

65. *In re Search Warrant Issued June 13, 2019,* 942 F.3d at 179 (citing adversarial hearings conducted concerning the DOJ's proposed use of filter team in the Michael Cohen matter, referenced *infra* Cmt. 8(c).

66. The UK Serious Fraud Office ("SFO") takes this approach, involving cooperation with organization counsel and review of search term responsive documents by independent counsel. R. (on the application of McKenzie) v. Director of the Serious Fraud Office, 2106 EWHC 102, 2016 WL 312261 (Admin) (Divisional Court, Jan. 27, 2016) (discussing procedures). Courts have criticized broad collections of privilege-rich ESI as is likely in a search of attorney files for their potential to irreparably damage the data rights of clients and of attorneys, as well as stressing the boundaries of probable cause needed in U.S. systems to support a judicial search warrant. In *In re Search Warrant Issued June 13, 2019*, the Fourth Circuit called out the government for the overbreadth of seizing entire mailboxes of attorneys without effort to

Screening of ESI may be conducted using computerized (often domain, name, or keyword) searches on-site in the collection process, or if the data is seized more broadly and is taken from the premises, screening may be performed by a third-party vendor or by agency staff with appropriate safeguards. The efficacy of these searches may be aided by input from the owner of the claimed privilege.[67]

Artificial-intelligence-driven technology may also aid in identifying and mitigating the risk of exposure of privileged information seized in a raid. Prosecutors who executed the search warrant of U.S. President Donald Trump's then-personal attorney, Michael Cohen, proposed that the ESI seized be assessed using Technology-Assisted Review software to identify potentially privileged documents, which would then be removed from the mass of data seized and separately reviewed by a special master. In this way, the burden on the review team and the risk of exposure to the prosecutors would be reduced. While the court hearing challenges to the seizure elected to proceed with a more traditional special-master procedure, it is foreseeable that the privilege screening process may be automated to a great

---

restrict the seizure just to the client at issue; ultimately, 99.8 percent of the 52,000 seized emails did not make any reference to the single client under scrutiny. 942 F.3d at 178. The Court rejected the assertion that review of such irrelevant material is required for "context" in making privilege determinations, as no probable cause exists to seize such documents. *Id.* (citing United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1172 (9th Cir. 2010) (en banc) (criticizing government "overreach" in seizure of electronic data unsupported by probable cause), abrogated on other grounds by Hamer v. Neighborhood Hous. Servs. of Chi., 138 S. Ct. 13, 16-17 (2017).

67. *McKenzie, supra* note 66 (in upholding SFO process of in-house technical staff isolating protected material, noting the "vast difference between the task of identifying a document as potentially attracting privilege and determining whether it was protected, a process which involved close consideration of the content and context.").

extent as technology improves and stakeholders become more comfortable with the process.[68]

Comment 5(d). *Privilege holders should take diligent steps to protect privilege across borders.* This principle also recommends vigilance on the part of those who have privilege claims to assert. While many jurisdictions (including the EU) will not impute a waiver to privileged advice seized during an inspection,[69]

---

68. Letter of Department of Justice to Hon. Kimba M. Wood (Apr. 26, 2018) (Case l:18-mj-03161-KMW) (S.D.N.Y.), *available at* https://archive.org/stream/Michael-Cohen-Court-Documents/2018-04-26-Cohen-28_djvu.txt. *See* FED. R. EVID. 502 explanatory note ("Depending on the circumstances, a party that uses advanced analytical software and linguistic tools in screening for privilege and work product may be found to have taken 'reasonable steps' to prevent inadvertent disclosure."). *But see* EDRM/DUKE LAW, TECHNOLOGY ASSISTED REVIEW (TAR) GUIDELINES (Jan. 2019) at 32 ("Privilege review is one area where existing permutations of TAR face significant challenges that may make them less valuable to clients and counsel.").

69. In general, the concept of waiver properly should not include involuntary or forced disclosures. *See* Facebook Interim Order, recital 103: "It should be noted in that regard that the applicant itself indicates, referring to the case-law of the United States courts (United States v. American Tel. and Tel. Co., 642 F.2d 1285, 1299 (D. C. Cir. 1980)), that such disclosure could only be characterized as a waiver in the case of a 'voluntary disclosure' of the documents at issue." Order of the President of the General Court in Case T-451/20 R, Facebook Ireland v Commission, EU:T:2020:515, at para. 62, *available at* https://curia.europa.eu/juris/document/document_print.jsf;jsessionid=D128683786B502FF27F2D433DF9CA36A?docid=233082&text=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=4350801. Defining what is "voluntary", however, may sometimes lead to debate, including whether reasonable steps were taken to protect such information from a raid. This lack of certainty is exacerbated in cross-border situations. Certain jurisdictions provide statutory and case-law protections. For example, Federal Rule of Evidence 502 limits the scope and effect of waivers associated with unintentional (involuntary) disclosures in certain U.S. proceedings, and even provides protections as to *intentional* disclosures in some circumstances. *See* FED. R. EVID. 502(d) (authorizing federal court to "order that the privilege or protection is not waived by disclosure connected with the litigation pending

this is not universal. Accordingly, privilege holders should aggressively seek to protect privileged information, even where such privilege is not always respected or clear.[70] As noted, documents seized in a raid and found not privileged in the home jurisdiction often make their way to jurisdictions like the U.S. with broader conceptions of privilege. (See Comment 6(d).) Among the factors a U.S. court will consider in evaluating whether such documents retain their privileged status in the U.S. are the efforts made by the organization to preserve the privilege, to object to each disclosure, and to retrieve the documents.[71]

---

before the court . . . [or] any other federal or state proceeding."); *id.* FED. R. EVID 502 explanatory note (protections available for "quick peek" situations where privileged information is provided to adversary, subject to retrieval). Parties subject to a dawn raid or collateral compelled disclosures may also consider requesting that the overseeing authority issue an order with findings of fact that the disclosure is not voluntary and does not waive any privilege or protection in any proceeding—although such order and findings would have uncertain impact outside of the authority's jurisdiction. A full discussion of the many ways that privilege information may be waived in interactions with authorities, and strategies to manage such risk, is beyond the scope of this *Commentary*.

70. The need for good-faith vigilance is heightened by the potential for prospective expansion or clarification of the scope of the attorney-client or legal-professional privilege by the courts. This was seen recently in the European Union Court of Justice's decision in Judgment of December 8, 2022, Orde van Vlaamse Balies, IG, Belgian Association of Tax Lawyers, CD, JU v. Vlaamse Regering, C-694/20, EU:C:2022:963, which clarified that the Legal Professional Privilege falls under the right to the protection of private communications, and so extends to attorney-client communications regarding legal advice beyond just those related to "rights of defense" in litigation.

71. *See In re* Parmalat Sec. Litig., No. 04-MD-1653, 2006 WL 3592936 at *5–6 (S.D.N.Y. Dec. 1, 2006) (denying plaintiffs' effort to use organization documents seized by Italian authorities from the organization's offices in Italy, even though the authorities broadly disclosed the documents, where the organization zealously and consistently asserted the privilege, judicially preserved its claims, and objected to disclosure).

Comment 5(e). *Protecting Privacy.* Digital assets and communication systems continue to proliferate, increasing the likelihood that personal data will be stored on an organization's systems, employee computers, and mobile devices seized by the authorities.

Authorities should therefore consider means to exclude irrelevant data identified as personal, particularly where employees designate data as such or make a request. The authorities may weigh several factors to help determine which safeguards for personal data are appropriate under the circumstances, including the investigative need, comity, and the privacy interests of implicated jurisdictions, subjects, and third parties. For example, if data has been seized from an organization in France, French employees' concerns might be given decisive weight if they have had no, or only peripheral, involvement in the subject matter of the inquiry. Conversely, if the investigation focuses on an individual's personal actions, the interests of conducting a thorough investigation might weigh in favor of including such content.

In many situations, the search can take a different approach when confronted with a directory that an employee has designated as containing personal content, or messages with indicative terms such as "PERSONAL" or "PRIVATE" in the header. Rather than blindly trusting such self-designations, authorities could search for agreed-to terms provided by the employee that can identify the specific content that should be excluded from the investigation; conversely, authorities could search a folder designated as "PERSONAL" for terms that would indicate only relevant (and nonpersonal) data. As stated previously, input from technical experts should be considered, and advances in technology hold promise for further automating this process.

Subjects of raids may advance this process considerably by taking appropriate steps to minimize their holdings of personal

information.[72] This is becoming increasingly difficult given the central role that electronic communication tools play in many employees' work life. Organizations may also wish to review their use policies—consistent with applicable law—to ensure they are clear as to how employees may use organization equipment/systems for nonbusiness purposes, and to note that companies may be required to disclose personal information to agencies without notice or direct remedial action.

Comment 5(f). *Protecting Sensitive Commercial Information and Trade Secrets.* Seized information transferred across borders and between agencies may include highly sensitive commercial information and trade secrets. The disclosure of such information may result in competitive harm or other harm to the subject in a manner that is not directly tied to the purpose of the investigation. Indeed, the investigation may have been precipitated by a competitor's complaint. In order not to inflict, even inadvertently, such collateral competitive harm or other harm on the subject of the investigation, transferring authorities should take reasonable steps to troubleshoot and protect the confidentiality and integrity of trade secrets against disclosures that may cause unfair competitive damage.

Similarly, even within the confines of a single jurisdiction, law enforcement agencies may have overlapping authority, and there may be requests, or even requirements, to share information gathered in a law enforcement investigation. In some circumstances, such recipient cooperating agencies may themselves be subject to requests to share information with their foreign counterparts. All such agencies in the originating country should take reasonable precautions within the scope of their authorities to ensure that any recipient of transferred information

72. *See generally* The Sedona Conference, *Commentary on Information Governance, Second Edition*, 20 SEDONA CONF. J. 95, 107, 129 (2019).

will protect sensitive commercial information and trade secrets from inappropriate disclosure.

Such restrictions in interagency transfers may include restrictive covenants appropriate for the nature of the transfer. Additional reasonable safeguards should be considered where such covenants are expected to be less reliable, for example, where political considerations are a factor or when transferring information to a foreign agency. In these situations, technical measures can be implemented to further protect the information. For example, the receiving agency can be invited to access the information through a secure online portal that provides the ability to access, search, and read documents, but restricts other functions such as printing or copying the information. Alternatively, the information can be protected with digital rights management tools, whereby documents are delivered but made accessible in a framework that blocks usage or transfer of the information and blocks access after an agreed period of time.

Finally, law enforcement agencies may themselves be subject to oversight, audits, and reviews by other authorities within their own nation. For example, within the U.S., the conduct of federal agencies, including (or especially) law enforcement agencies, are commonly subject to inquiries by various Congressional committees, the Government Accountability Office, the Office of Management and Budget, and Inspectors General, among others. Where those oversight bodies assert an absolute right to have access to all information in an agency's possession, those oversight authorities should use extreme diligence before disclosing their collected information, whether directly or in their "Final Reports," that may inflict collateral damage on private parties or investigative targets, domestically or internationally.

Comment 5(g). *Out-of-Scope Uses of Protected Information*. Where information subject to foreign data protection laws has been obtained in a raid through agreement or cooperation of the locality, the information should be used only for permitted purposes, as discussed under Principle 6. While agreement on this issue should be established between the governments in advance of the transfer, to the extent it is unaddressed, the authority in possession should seek additional agreement of the foreign sovereign before transferring the information onward or using the information for uses other than its authorized purpose.[73]

Comment 5(h). *Handling of Documents at the Close of an Investigation.* Like every other organization, law enforcement agencies need to record their actions and maintain records of their decision-making. Such requirements, even when they are not imposed by laws such as the Federal Records Act in the U.S., are well-grounded in practical necessity. Law enforcement agencies need to have an "institutional memory" of their actions; they need to be able to identify and learn from their past experiences; and they need to be able to account for their actions with their own supervisory authorities.

When investigations end, law enforcement agencies are not always able to return or destroy all the information they have

---

73. *See* USJM, *supra* note 10, § 9-13.512 (Intended Use of the Evidence) ("When a country provides evidence pursuant to a request for legal assistance, such as an MLAT, letter rogatory, or letter of request, contact OIA [Office of International Affairs] before using or disclosing it for a purpose other than that specified in the legal assistance request. (Examples of such use or disclosure include Freedom of Information Act requests, or requests to use the evidence in a parallel civil or administrative proceeding.) OIA will work with the USAO [U.S. Attorney's Office] to determine whether the evidence can be used for a different purpose without the express permission of the country that provided it and, if not, for guidance in securing such permission.").

collected. It may also be assumed that information that is not needed for any purpose other than record keeping may be subject to loss, theft, misuse, inadvertent disclosure, and other mishaps. Each of those outcomes can cause direct and immediate harm to the subject of the investigation and to disinterested third parties that may have been brought into the investigation for one purpose or another.

To mitigate these risks, authorities therefore should take reasonable steps to return or destroy all collected information and related materials that reflect the contents of such documents, except to the extent they are required to keep them for mandatory record keeping purposes and for the on-going operations of the authority. To the extent any such remaining records are not subject to mandatory disposition schedules, they should be reviewed at periodic intervals with the goal of disposing of all materials that the agency no longer needs. The agency should not wait until the end of the case to return seized materials deemed unreviewable on the ground of privilege; such data should be returned at the first opportunity after such determination (as well as kept in a secure environment in the meantime). An agency should also be receptive to requests of the former holders/owners of the data for an updated inventory or accounting of what data is being retained, and the basis for continued retention.

Many agencies now keep their records in the cloud, which in theory makes disposal easier. However, special note should be made of backup systems and other redundant copies of documents and related information, such as office or personal "convenience" copies that investigators may have kept. Although it may be impractical to suggest that backup tapes should be systematically opened and reviewed at the end of each investigation, this *Commentary* suggests that they be kept on a strict disposition schedule that allows for their destruction at a time when "more recent" backups would be sufficient to reconstruct

agency activities in the event of any disastrous loss or other operational need. Similarly, individual investigators should be encouraged, or required, to periodically (at least annually) review their files and dispose of all unneeded materials.

B. Principles and Best Practices for Those Subject to Dawn Raids

Principle 6: Organizations and third parties subject to a dawn raid should cooperate in the raid and should not obstruct or otherwise impede its conduct. On the other hand, the mere assertion of rights and attempt to exercise those rights should not be considered lack of cooperation or obstruction.

Comment 6(a). *Cooperation with authorities and lawful instructions.* Organizations and individuals involved in raids should—and generally are obligated to do so by law[74]—cooperate, avoid obstructing, and comply with authorized and reasonable requirements of inspectors conducting the raid. Cooperation, moreover, can be effective strategy in minimizing damage and mitigating risk of such raids.

Comment 6(b). *Consequences for lack of cooperation.* The potential consequences of the failure to cooperate are severe. First, the authority may levy significant fines or bring or make a referral for criminal charges against the organization/actors for obstruction of the investigation. For example, the EC is empowered to issue a fine of up to 1 percent of the total turnover in the preceding business year for noncooperation and incomplete cooperation, and up to 5 percent of the average daily turnover in

74. For example, the UK Competition Act 1998 Sec. 70 makes it an offense to hinder, oppose, obstruct, or unduly influence any person exercising a power or carrying out a duty in terms of the UK Competition Act, https://www.legislation.gov.uk/ukpga/1998/41/contents.

the preceding business year for each day that an organization does not permit inspection.[75] Obstruction may also be considered an aggravating circumstance in issuing sanctions for violating EU rules of competition[76] and separately may be considered a criminal act.

Comment 6(c). *Conduct constituting obstruction.* Determining what conduct crosses the line for failure to submit to inspection is highly fact-specific, but certain actions will create risk. One of the first things that inspectors look for is the deletion or failure to take appropriate steps to preserve data during the pendency of the investigation. Cooperation should always include preserving information within the scope of the authorizing instrument. Critical first steps include suspending any auto-delete programs and notifying personnel of the need to preserve relevant documents and data. The organization should also consult

---

75. The UK Competition Act, *id.*, Sec. 28; EU Competition Regulation 1/2003, *supra* note 3, Arts. 23 and 24. *See also* Directive (EU) 2019/1 of The European Parliament and of the Council of December 11, 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, Art. 16 (The ECN Plus Directive requires the imposition of "effective, proportionate and dissuasive fines" for hindering a raid), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0001.

76. *E.g.*, *Dawn Raid Derailment—A Cautionary Tale*, JONES DAY (Oct. 16, 2018), https://www.jonesday.com/en/insights/2018/10/dawn-raid-derailmenta-cautionary-tale (cataloging fines: in 2018, EC administrative finding of obstruction against Slovakia's state-owned railway ZSSK for hiding, and then overwriting, data on a laptop requested by officials during inspection; in 2015, the General Court of the European Union ("GCEU") upheld an EC fine of 2.5M euros against Energeticky and its subsidiary for circumventing inspector-required IT lockouts of employees to email accounts and diverting additional email from inspectors' attention; in 2012, a GCEU ruling affirmed a 10 percent increase in fine on Koninklijke Wegenbouw Stevin ("KWS"), which refused access to Commission officials until KWS's attorneys arrived almost an hour later and refused temporarily to provide access to a director's office based on the assertion it contained no relevant information).

with legal counsel as to the extent of its additional preservation obligations relevant to the investigation and update the scope of preservation based on subsequent developments, including the results of further interactions with the authorities and the organization's own investigation.

Once premises are sealed by inspectors, breaking the seal is subject to criminal penalties, including incarceration and significant monetary fines.[77] The failure to comply with inspector instructions regarding access to information may also be viewed as lack of cooperation. Examples include: the failure to provide passwords (including failing to cooperate in providing biometric identifiers) and to decrypt data; taking steps to divert relevant incoming information; and failing to provide remote (including cloud) access. One live issue is whether and under what circumstances inspectors may demand access to information maintained in a foreign jurisdiction. (See Comments 7(a)-(b).) For example, in 2019, the Turkish Competition Authority issued obstruction fines to Unilever and Siemens purely for not giving access to cloud storage. No data was lost, and granting access would likely have violated the European Union's General Data Protection Regulation (GDPR), suggesting that organizations may want to consider whether their systems should be designed

77. Under EU rules, the EC may "seal any business premises and books or records for the period and to the extent necessary for the inspection," EU Competition Regulation 1/2003, *supra* note 3, Art. 20(2)(d). "The Commission may by decision impose on undertakings . . . fines not exceeding 1% of the total turnover in the preceding business year where, intentionally or negligently . . ., seals affixed . . . by officials or other accompanying persons authorized by the Commission have been broken." *Id.*, Art. 23(1)(e). In 2010, the GCEU affirmed the EC's decision to impose a €38 million fine on the German energy provider, E.ON, for breaching an area sealed during a dawn raid. *Antitrust: Commission welcomes General Court ruling on E.ON breach of seals case* (Dec. 15, 2010) https://ec.europa.eu/commission/presscorner/detail/de/memo_10_686.

to provide only limited access in order to shield data residing in other jurisdictions.

Comment 6(d). *Additional factors in cooperation.* The manner in which an organization responds to a dawn raid may also have an impact on the authority's perception of the subject. The U.S. Department of Justice, for example, may consider conduct deemed uncooperative as evidence for separate charges of obstruction as well as a factor in determining cooperation credit in sentencing.[78] Certainly, prosecutors have a way of making life harder for organizations perceived to be hindering an investigation.

Comment 6(e). *Cooperation obligations of third parties.* A third party on site in a dawn raid shares obligations of the subject to cooperate and not impede the execution of the raid. To the extent that the third party is under the control of the subject, moreover, any obstruction or failure to cooperate may be attributed to the subject. The subject organization should make sure to educate such third parties under its control about raids and their rights and obligations. For example, a third party may have been engaged by the organization to manage its IT resources and may be asked to provide access to systems or even sit for interview. Another scenario may involve an independent third party (such as a customer) who is onsite during the raid, or whose information or property is caught up in the raid. Such independent third parties would be well counseled to not impede the execution of the raid, although their affirmative obligations are unclear.

---

78. John Davis and Tom Hanusik, *New DOJ Policies Relieve "Catch-22" Pressure on Companies Conducting Cross-Border Investigations*, CROWELL & MORING (Dec. 14, 2018), https://www.crowell.com/en/insights/client-alerts/new-doj-policies-relieve-catch-22-pressure-on-companies-conducting-cross-border-investigations.

Comment 6(f). *Legitimate assertions of rights should not be the basis for a finding of non-cooperation.* For example, there should be a process where the target of a raid may in good faith challenge the request of an EC investigator to take a "cursory look" at files to which a privilege claim is asserted. This process would allow for verification of the basis of the privilege assertion by an objective reviewer before the harm of even "cursory" disclosure occurs. Under this process, the agency should not rely upon such assertion of rights as a basis to fine or otherwise penalize the target, even where such objection is subsequently determined to lack merit. Moreover, consistent with Principle 1, any such determination should be made by an independent authority, and not the authority that is seeking the disclosure. Note, however, that some authorities may view perceived abuse of such challenges as obstructive behavior.

Principle 7: Organizations should assess the risk of dawn raid occurrence, including to the business, contracts, and protected information, and take reasonable steps to prepare for and mitigate such risks.

Comment 7(a). *Organizational steps to assess and mitigate data risk.* To properly manage a dawn raid, organizations should take appropriate steps to assess their risk and impact, understand the organization's rights and obligations, and use that information to prepare for their occurrence and mitigate their effects. First steps include:

- Developing and implementing written dawn raid procedures with clear allocation of responsibilities;
- Practicing responding to raids to minimize impact on the organization and impacted information; and

- Taking steps to safeguard information at risk of unauthorized access and disclosure (e.g., storing privileged information in clearly labeled, secure areas).

Annexed hereto is a checklist of best practices that may be used by organizations in preparing for and responding to data privacy and cross-border issues in dawn raids. The following discussion of issues provides a framework for considering and implementing the checklist of best practices:

Comment 7(b). *Data protection.* Information at risk of a raid may be subject to a variety of protections based on access, location, content, or usage. It is therefore necessary to evaluate the nature of the data that may be seized and the protections that could apply. This can be assessed by answering the following questions:

- What jurisdictions' laws apply?
- Do those laws apply to this data?
- What do the laws restrict?
- Do any exceptions apply?
- What measures should be taken to comply with the law?
- Which offices or operations of the organization need access to this data?
- Should steps be taken to limit access to certain data in certain countries?

Organizations should address these issues in advance of a raid, given the difficulty of attempting to do so in the moment.

Protections that may come into play include those regarding banking information (e.g., Swiss Banking Act Art. 47) and other protections that may apply if the authority is foreign to the targeted organization, such as sovereign protection or "blocking" statutes (e.g., Swiss Penal Code Articles 271 and 273) and state

secrets laws (e.g., China State Secrets Act).[79] While the GDPR[80] would not limit the powers of an investigating agency, the organization should be mindful of personal information covered by the GDPR and take steps to safeguard against *any* sort of unauthorized disclosure.

Comment 7(c). *Legal Privilege.* It is outside of the scope of this *Commentary* to survey global privilege law,[81] but it is clear that

---

79. *See also* French Law no. 68-678 of July 26, 1968, relating to the Communication of Economic, Commercial, Industrial, Financial or Technical Documents and Information to Foreign Individuals or Legal Entities, as modified by French Law no. 80-538 dated July 16, 1980, Art. 1 ("Subject to treaties or international agreements it is prohibited for any individual of French nationality or who usually resides on French territory and for any officer, representative, agent or employee of an entity having a head office or establishment in France to communicate to foreign public authorities, in writing, orally or by any other means, anywhere, documents or information relating to economic, commercial, industrial, financial or technical matters, the communication of which is capable of harming the sovereignty, security or essential economic interests of France or contravening public policy, specified by the administrative authorities as necessary [emphasis added]."); *id.* at Art. 1b ("Subject to any treaties or international agreements and the laws and regulations in force, it is prohibited for any person to request, to investigate or to communicate in writing, orally or by any other means, documents or information relating to economic, commercial, industrial, financial or technical matters leading to the establishment of proof in light of foreign administrative or judicial proceedings or as a part of such proceedings."); *id.* (permitting foreign disclosures conducted under international agreements or treaties); French Law no. 2016-1691 (Sapin II Law) (requiring the Agence française anticorruption to ensure compliance with blocking statute by organizations, under investigation by foreign authorities, that have entered into agreements requiring the appointment of a corporate monitor).

80. In general, privacy protections will not preclude authorities' access to information seized in a raid. That does not, however, end the headaches that may ensue for organizations dealing with the aftermath of a raid.

81. *See generally Sedona Cross-Border Privilege Commentary*, *supra* note 8 An interesting overview of the Legal Professional Privilege before EU Courts in competition proceedings is set out in the OECD LPP Report, *supra* note 59.

protections for legal privilege vary significantly across jurisdictions. For example, as a general proposition, the attorney-client privilege may be strong in the U.S., less so in the UK, and largely inapplicable in many other nations. Organizations should educate themselves as to privilege rules applicable to their information, as well as the procedures in place that authorities apply to privileged information in dawn raids.[82] Organizations should also put in place a protocol to determine how to manage privileged content, particularly when data is removed from the organization. Further, organizations should proactively engage with regulators to understand and influence the process. This should take the form of advising the regulatory agency of the names of all in-house and outside counsel, as well as law firm names, and to the extent known, particular issues and areas that counsel has been consulted on and that may be privileged.

In addition to the process afforded by the authority, organizations should conduct their own privilege examination of seized information. An organization's failure to be diligent in reviewing its own files and promptly raising privilege objections may be seen in some jurisdictions as a lack of concern about authorities' use of the privileged information and lead to negative outcomes. (See Comment 8(d).)

Comment 7(d). *Confidentiality.* Organizations similarly should seek to have a protocol put in place to manage confidential information for the whole lifecycle of the investigation. The protocol should specify the conditions under which a document will be deemed confidential, and the requirements for preserving confidentiality.

Comment 7(e). *Security.* Although security often is assumed when a governmental body seizes data, organizations must

82. *See* INVESTIGATIVE POWERS REPORT, *supra* note 19, § 2.5 (discussing variations of process for protecting legal professional privilege during raids).

familiarize themselves with security conditions during and after the raid. As noted, organizations should implement security protocols for the whole lifecycle of the investigation, enable a secure investigation environment, and confirm encryption for data in transit. Among the ways to promote security are to: ensure that the search is consistent with the scope of the warrant; consider objecting to disproportionate searches (such as wholesale collections and forensic images of laptops); and follow up on data return/destruction at the appropriate time.

Comment 7(f). *Third-party rights.* Third parties' protected and sensitive information and property may be caught up in a raid in the same manner as those of the subject. While authorities are generally bound to confidentiality and may return seized data following completion of the investigation, they may also share seized information with other regulators in certain circumstances.

Third parties should consider the legal and contractual obligations of the data controller to their information, including to notify the third party of a seizure and to cooperate in ensuring that appropriate steps are taken to obtain an accounting and to protect such information.

Notice requirements vary according to jurisdiction, parties, and subject matter. In general, authorities have no obligation to notify data owners of seizures. Similarly, it is likely that a transfer of protected information to an authority in a dawn raid or through subsequent legal means would not constitute a breach of data protection regulations or require notice by the organization. For example, there is no requirement under the GDPR that organizations notify persons whose personal information was seized by the EC or EU authorities in a dawn raid, although non-

EC/EU authorities are outside of this safe harbor.[83] There may, moreover, be contractual or prudential reasons for notice.[84]

---

83. *See* Letter of EDPS assistant supervisor Wojciech Rafal Wiewiorowski, Subject: Investigative activities of EU institutions and GDPR (Oct. 22, 2018), https://edps.europa.eu/sites/edp/files/publication/18-10-30_letter_investigative_activities_eui_gdpr_en.pdf (while GDPR Article 14(1)(e) requires controllers to inform data subjects about the "recipients or categories of recipients" of their personal data, GDPR Article 4(9) specifies that "public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients," and so no notice is required).

84. Further question as to governmental authorization and notification is raised when evidence is seized by nonstate actors with judicial authorization to conduct forced, no-notice inspections similar to dawn raids. One example is a counterfeit search and seizure action (*saisie contrefaçon*) initiated through an ex parte request of a court by the owner of an intellectual property right. Upon a sufficient showing, a court may authorize an independent expert or supervising solicitor (sometimes backed by locksmith, police, party solicitors, and technicians) to conduct an unannounced inspection on the infringing party to obtain evidence confirming the infringement. *See* Jan-Diederik Lindemans, *Transatlantic "Hide and Seek": Proving Infringement of Intellectual Property Rights through Pre- Trial Proceedings for Taking Evidence in the United States and the European Union*, E.I.P.R., Issue 8 pp. 455-62 (2013), https://fordhamipinstitute.com/wp-content/uploads/2015/11/Sunrise-III-2-Lindemans-Jan-Diederick.pdf. While not a dawn raid, similar private remedies may raise similar data privacy and protection issues and are available in a variety of jurisdictions, including the UK and other common law countries (*e.g.*, Anton Pillar orders, which more closely resemble contempt proceedings), other EU nations, and the U.S. (*e.g.*, Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, Art. 7, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004L0048R%2801%29; 17 U.S.C. § 503(a); *see also* 18 U.S.C. §1836(b)(2)(A)(ii) (authorizing court under the Defend Trade Secrets Act to issue an ex parte order enabling the seizure from defendants of "property" containing plaintiffs' trade secret information; utilizing law enforcement to take possession of data, documents, and repositories identified in the order as containing such information; and the appointment of neutral technical experts to facilitate such seizure).

Organizations, however, are cautioned to consider coordinating any such notice with authorities, as giving notice may be viewed as interfering with the investigation by tipping off other suspects. As previously noted, obstructive conduct has reinvigorated many an investigation that had already gone stale on the merits.

> **Principle 8:** Organizations should assess their response to a raid and consider any mitigation and remediation steps appropriate to protect their data rights and those of third parties that are affected by the raid, and to improve future responses.

Comment 8(a). *Post-Raid Challenges to Actions*. Issues with the authorization, scope, conduct, and implications of the raid may be evident from the beginning. The organization should be familiar with the grounds to challenge such raids in court, including to move to block follow-on raids and require protections and restrictions on the use of the information obtained. Organizations may have an advantage if they strategically deploy knowledgeable counsel to shadow investigators, understand investigators' search strategies and how they conform to scope as defined in the inspection decision, and ensure that investigators follow procedure and respect privilege. While authorizing instruments are often so high-level and broad as to frustrate efforts to rein in overbroad search and seizures, it is critical to assert objections in real time and insist that they are recorded in the minutes of the raid.[85] As discussed below, further

85. The European Court of Justice's decision in *Deutsche Bahn AG and Others v. European Commission* (Case C-583/13 P) (ECJ 2015) illustrated the utility of such practice. Among the factors that the court looked at in determining whether out-of-scope evidence was seized in a raid through a permissible "accidental" discovery or an impermissible "targeted search" are the

investigation may also uncover additional support for or reason to assert such challenges.

Comment 8(b). *Post-Raid Assessment: Initiate an Internal Investigation.* At its earliest opportunity, the organization will want to understand the scope and purpose of the investigation, and the underlying facts. The first step is to determine what records and data have been seized and undertake an internal investigation into the underlying conduct. The goals of the internal investigation are two-fold: first, to understand the organization's exposure and options, including whether it has an obligation to self-report or may want to come forward for purposes of earning cooperation credit; and second, what, if any, obligations and rights the organization has in relation to the seized records and data.

As to the first goal, the internal investigation should be conducted in order to understand substantive and other risks to the organization from the agency conducting the raid, from other regulators with whom the authority may share its information, and from competitors who may have filed a complaint to spur the raid or were alerted to the raid or the investigation. For instance, it is possible the agency conducting the raid may share information seized with other agencies in its own government or with foreign governments if the investigation is a multistate investigation. The internal investigation will often proceed beyond the information seized. For raids conducted by a competition authority, the organization will urgently want to reach a conclusion about the potential for an application for leniency. Success may be measured in days, hours, or even minutes, where credit is granted to early actors.

---

contemporaneous minutes of the search. A subject's after-the-fact reconstruction of what occurred may be viewed as less credible.

As to the second goal, to the extent that the investigation identifies data from third parties that has been seized in the raid, the organization will need to assess its obligations to those parties. Those obligations may include giving notice and an opportunity to intervene, consistent with confidentiality requirements, if any, that may apply under the circumstances of the raid and the larger investigation.

Comment 8(c). *Maintaining Privilege.* Typically, the organization should engage experienced outside counsel to conduct the investigation, thus maximizing the extent that the investigation is covered by lawful privilege (noting that privilege protections may vary from jurisdiction to jurisdiction). While the organization may ultimately decide to waive any privilege to present results of the investigation in return for leniency, without proper planning, there may be nothing to waive. Additionally, government agencies may disfavor an investigation conducted solely by the internal resources of the organization that is under investigation, as they may be perceived to lack independence. Thus, this *Commentary* recommends engaging outside counsel, and more specifically, outside counsel without substantial other business with the organization, such that the investigation, and its work product, will be viewed as independent and objective.

Outside counsel should consider hiring an independent forensic IT consultant to conduct the on-the-ground investigation as to what data and records were seized. Again, this puts an objective outside expert in the position to record and assess what was seized, what remains, and to what extent other relevant materials are available and may need to be produced. As discussed above, it is critical to expedite this review by compiling a comprehensive record of all data and devices seized during the raid and retaining copies when possible.

Comment 8(d). *"Clean-Up" Subpoenas*. In the U.S., the government team executing the search warrant will often serve a grand jury subpoena in connection with the dawn raid as insurance for obtaining all relevant data and records, including records and data that the team may have missed in the search. If the government agency does serve a subpoena or civil investigative demand in connection with or after the raid, it becomes even more important to determine through an internal investigation what materials have been seized and whether materials that have not been seized are nonetheless subject to production to the government under the subpoena. The timeframe for a response will typically be very short. In order to fully comply with the subpoena, the internal investigator may have to examine laptops and mobile phones of employees who were not present during the raid or who work remotely, backup servers, cloud-based data, and other data sources that were not subject to search. Even absent a subpoena or investigative demand, the organization should authorize the investigative team to fully explore potentially relevant sources of documents and data in order to have a complete understanding of the organization's potential exposure.

Comment 8(e). *Notification and Dawn Raid Plan for Other Facilities/Locations.* The organization should also consider the possibility of further raids—for the instant investigation and any later investigations—and how best to respond to make such raids less disruptive and risky to the organization. Such response must be consistent with legal obligations, including cooperation and preservation obligations in relation to the investigation.

If the organization does not already have a dawn-raid policy in place, it should consider creating and implementing such a policy as quickly as possible and distributing it to other facilities and locations. Elements of a dawn-raid policy are set out in the Appendix hereto. The organization, working in concert with

outside counsel, should analyze whether there are obvious facilities and locations for a follow-on raid, and, to the extent possible, pre-position legal assets on location to be prepared to respond. For example, some organizations should make sure to have in place several high-volume portable storage devices to make a contemporaneous copy of all data transferred to the authority.

The organization should also consider the following proactive data control steps:

- Organizing information in a manner more conducive to cooperation so that any additional search will be less disruptive to the organization;
- Understanding and evaluating the extent, use cases, and limitations on cross-border access to information in protected jurisdictions;
- Strengthening access controls and need-to-know policies;
- Implementing encryption and digital rights management software;
- Limiting proliferation of information across locations/jurisdictions; and
- Maintaining encryption keys locally, so that seizure or point of access in one location does not compromise security elsewhere.[86]

---

86. The organization must ensure that any such steps are consistent with its cooperation obligations, including to not inappropriately hinder an investigation and to preserve data sought and of relevance to the investigation. *See supra* Cmt. 1(c). Switching to ephemeral messaging in the midst of an investigation with ongoing preservation obligations, for example, will likely be viewed negatively through the prosecutorial lens. *See, e.g.*, FTC v. Noland, No. CV-20-00047-PHX-DWL, 2021 WL 3857413 (D. Ariz. Aug. 30, 2021) (sanctioning defendants that, the day after learning of government investigation, switched to the Signal ephemeral messaging platform and set all

Comment 8(f). *Advice to Employees—Potential Approach by Investigators.* A critical part of the organization's response is to prepare its employees for the possibility that they may be contacted by government authorities as part of the post-raid investigation. The best practice is to instruct employees how to conduct themselves before a dawn raid occurs; mock dawn raids and practice dry runs may help. Employees should be advised of their rights and responsibilities, both in terms of the substance of the investigation and any requests government agents might make for records or data within the employee's care, custody, or control. The investigating agency may even move to execute searches at the homes of individuals, including employees, owners, directors, and, in some cases, legal counsel.

In general, employees that are approached by investigators have the following rights and responsibilities. **Organizations should confirm consistency with local governing law**.

- The employee has the right to know that there is an investigation that relates to particular issues as described;
- The employee has the right to speak with an investigator;
- The employee has the right not to speak with an investigator to avoid providing potentially self-incriminating answers;[87]

---

messages to "auto-delete," finding they intentionally deprived agency of relevant documents); Herzig v. Ark. Found. for Med. Care, Inc., No. 2:18-CV-02101, 2019 WL2870106 (W.D. Ark. July 3, 2019) (finding that use and "necessity of manually configuring [the messaging app] Signal to delete text communications" by plaintiffs was "intentional and done in bad faith").

87. *See* Judgment of 2 February 2021, DB v Commissione Nazionale per le Società e la Borsa (Consob), C-481/19, ECLI:EU:C:2021:84. (recognizing that the EU Charter of Fundamental Rights provides for a right to remain silent for natural persons in administrative investigations; precluding penalties for

- The employee has the right to speak with the investigator with counsel present;
- The employee should be courteous and professional at all times.
- If the employee speaks with an investigator, the employee should tell the truth in all respects and should not guess or speculate as to any matters;
- The employee should not take any action to destroy, delete, edit, or modify any records or data in the care, custody, or control of the employee;
- If the employee is asked to provide organization documents or data or is asked to provide access to organization IT platforms, the employee should not refuse the directive but may request that the investigator instead direct the inquiry to counsel for the organization;
- If the employee does have relevant records or data in its care, custody, or control, the employee should notify organization counsel or the investigation team immediately; and
- If an employee is approached by an investigator, the employee should notify the organization's counsel or the investigation team of the contact immediately.

Of course, nothing in the advice to employees should suggest in any way that the employee may obstruct or impede the investigation. That said, the organization *normally* is entitled to notify its employees that the investigation is ongoing and to advise employees of their rights and responsibilities. In appropriate circumstances the organization might consider offering to

---

persons who refuse to provide potentially self-incriminating answers to investigating authorities under EU Directive No 2003/63 and EU Regulation No. 596/2014.4).

provide independent, individual counsel for some or all of its employees. There may, however, be particular investigations where disclosure is forbidden (e.g., relating to national security) or discouraged (e.g., where prosecutors wish not to tip off persons).[88]

Comment 8(g). *Remediation*. The internal review following a raid may uncover issues that the organization wishes to address independent of the underlying investigation, e.g., violations of legal, contractual, and organization requirements; inefficiencies; failures to follow best practices; difficulties in responding to the raid; compliance weaknesses; IT weaknesses; and information management gaps. The internal review may provide the necessary information for the organization to both proactively address data and records issues highlighted by the dawn raid

88. Indeed, authorities may view paying for counsel for employees to be evidence of noncooperation or obstruction if the payment appears conditioned on adherence to facts that the authority believes all involved know to be false. The DOJ previously took an even more extreme position on this. In the now-withdrawn "Holder memo," the DOJ indicated that in some circumstances "a corporation's promise of support to culpable employees and agents, either through the advancing of attorney's fees, [or] through retaining the employees without sanction for their misconduct . . . may be considered by the prosecutor in weighing the extent and value of a corporation's cooperation." Memorandum from Eric Holder, Deputy Att'y Gen., to all U.S.D.O.J. Component Heads and U.S. Att'ys (June 16, 1999), *available at* https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2010/04/11/charging-corps.PDF. The DOJ now expressly disclaims reliance on whether an organization is paying its investigated employees' attorney fees or providing them counsel, while still holding that "[i]f the payment of attorney fees were used in a manner that would otherwise constitute criminal obstruction of justice—for example, if fees were advanced on the condition that an employee adhere to a version of the facts that the corporation and the employee knew to be false—these Principles would not (and could not) render inapplicable such criminal prohibitions." USJM, *supra* note 10, § 9-28.730.

and confront the underlying matters that are the subject of the investigation.

Comment 8(h). *Disclosures*. Some of the most complicated issues that arise in the aftermath of a dawn raid are whether and how to disclose the fact of the raid, the larger investigation and remediation, and what data was collected. The post-raid review should be the starting point for these issues.

Potential disclosure targets include insurers, auditors, other regulators, contract parties, and the market, as well as third parties whose proprietary, restricted, or personal information has been seized during the raid. Authorities conducting dawn raids are generally operating under appropriate exceptions as to transfer and processing of personal/restricted information. However, there may be contractual and other obligations, as well as business imperatives, to notify customers and other third parties whose information has been seized or implicated in the investigation. One difficult determination is how to approach making disclosures to stakeholders whose data may have been collected by the investigating body. Especially in a climate of increased sensitivity regarding data privacy, there may be reasons to consider telling customers that their personal data was seized by the government during a raid.

Further, if the organization were to determine after the fact that personally identifiable information that was nonresponsive to a subpoena was collected, the organization could work with the government to seek appropriate redactions or, if necessary, challenge the storage and review of the material. These efforts are often unsuccessful in criminal investigations, especially in the U.S.,[89] but could lend credibility to rebuttals of any possible

89. *See, e.g.*, United States v. Davis, 767 F.2d 1025, 1033–34 (2d Cir. 1985) (siding with the DOJ in a challenge to a criminal investigation on comity grounds).

future allegations that the organization failed to take adequate steps to safeguard personal information, as well as bolster corporate efforts to demonstrate concern for customer privacy.

APPENDIX: ORGANIZATION CHECKLIST IN PREPARATION FOR DAWN RAIDS

While a chronological structure can be effective, ensuring that the response is functional under the pressure of a dawn raid is paramount, and preparation could be structured as follows:

- Pre-Raid Preparation: Sections on introduction, roles and responsibilities, legal rights and obligations, and training and rehearsals. This part focuses on the groundwork and readiness before any raid occurs.
- During the Raid: Starting with immediate actions upon the arrival of investigators, followed by detailed procedures for document handling and communications. This part is structured around the sequence of events typically occurring during a raid.
- Post-Raid Follow-Up: Focused on the aftermath of the raid, detailing the debriefing process, legal follow-up, and any necessary adjustments to the plan based on lessons learned.

When preparing, keep the following checklist in mind:

1. **Policies**

    a) A formal, written policy should be developed for dealing with dawn raids and customized to the location in advance.

    b) That policy should include at minimum:

        1) Detail immediate tasks to be undertaken during a dawn raid.

        2) Identify responsible persons (e.g., reception, head of building or plant, IT, head of communications, and in-house counsel).

3) Identify pre-engaged outside counsel and IT, electronic discovery, and/or forensic vendors.

4) Provide detailed actionable material (e.g., a Dawn Raid Plan) that is rolled out and available at all times.

5) Document procedures on data preservation and collection, including privacy and legal-hold notifications.

6) Ensure updating and enforcement of data retention, hygiene, access, and usage policies.

7) Ensure updating and circulation of email/communications channel usage policies (including those regarding marking, storing, and sharing privileged documents) and use/privacy notifications.

8) Evaluate heavily regulated and highest risk operations, as well as high-risk jurisdictions and location.

2. Actionable Materials – Dawn Raid Plan

A dawn raid plan should contain:

a) Detailed instructions and be tailored to each member of the dawn raid team.

b) Up-to-date contact information of all responsible persons, including designated dawn raid team members responsible for coverage of a certain location.

c) Up-to-date contact information for all outside counsel and IT, electronic discovery, or

forensic vendors, and which location they are servicing.

d) Detailed instruction at reception at all relevant locations, including the relevant contact information for that location, along with a communication and action protocol in place that describes exactly what information the receptionist should provide and what actions the receptionist should take.

e) IT capabilities that include a computer with controlled access to needed systems.

3. Dawn Raid Team Roles and Responsibilities

Create a designated dawn raid team. Members should be the first responders in the event of a dawn raid. In larger or international organizations with many locations, it is advisable to establish local teams as well as a central directing team. The following roles are typically needed during a dawn raid and should be established in advance:

a) Team leader: One person should be the team leader. The leader is the face of the organization to the authorities, and, preferably, the decision maker for all actions taken during the dawn raid. He or she instructs all team members. Often the team leader is an in-house counsel or executive working with advice of outside counsel.

b) In-house counsel: In-house counsel must be educated as to the rights and limitations of the actions of authorities and the organization's options to object, as well as be responsible for managing the process and challenging

inspector actions. They should study the subpoena/warrant or operative document and set limits regarding the inspection based upon the rights of the inspector and the documents. Legal objections should be lodged if appropriate.

Questions should be asked in real time when the inspectors' actions appear to exceed scope or threaten privilege/protection (e.g., collection requests or search terms overbroad in context).

c) Outside counsel: Ideally, outside counsel will be preselected and engaged in relation to the type of inspection (e.g., antitrust) and data issues involved, and available on call and able to service a specific location within a reasonable time. Outside counsel will generally have the same function as in-house counsel, including specific expertise and experience with dawn raids.

d) Communications lead: One person should be the face of the organization to the news media. The communications lead should rely on predrafted statements and communicate only in consultation with in-house and/or outside counsel. Consider whether a public relations consultant should be engaged.

e) Additional team members: Typically, additional team members are compliance officers, data security officers, or other trained personnel from the organization who will accompany inspectors as they fan out. They will document all actions, including documents viewed or

taken, persons questioned, questions asked, etc. Team members will frequently inform and align with the team leader.

f) IT expert: An IT expert (e.g., someone with a background in operations, electronic discovery, and/or forensics and is experienced in working with counsel on legal matters) and at least one designee are needed to ensure that the inspector's questions regarding the organization's data storage practices and policies can be answered (including directing inspectors to required data stores and noting where and how privileged/restricted items are kept).

The IT expert plays a crucial role in scoping data collection and should be knowledgeable enough to make educated suggestions on how to accurately guide the inspector's requests. It is critical that the IT expert can identify, preserve, and ultimately collect required data to make it available to the inspectors and to document and retain a copy of all data provided for the organization (remote support may be required).

This goal may be achieved in several ways, such as:

1) Large-capacity hard drives can be filled with data that is subject to seizure by the inspectors, so the inspectors may take a copy and the team may also keep a copy of exactly what was taken. If there is no ability to keep a copy of what the inspectors seizes,

consider asking the court to resolve the issue.

2) Other systems may allow for preservation in place or require longer time to collect, giving the organization time to deliver the required data after the dawn raid. The IT expert should be ready to discuss options of how to deliver data to inspectors in the days after the dawn raid.

g) Forensic specialist: This team member, whether internal or external, should be preselected to assist as needed.

h) Receptionist: Receptionists are typically the first contact and should obtain a copy of the warrant and check its legitimacy and the inspector's identification. Receptionists play a critical role in greeting the government team, timely informing the organization's dawn raid team, especially outside counsel on call, and guiding inspectors to a designated area.

i) Plant security and/or facility management: Plant security may shield off inspectors from regular operations and reroute employees and customers. Plant security will provide access for inspectors under the dawn raid team's supervision while maintaining overall security and confidentiality. Plant security may also be helpful in providing support and supplies as needed (e.g., additional office space, office supplies, chargers, food and water, keeping the facility open after hours as needed, etc.).

4. Training

a) The dawn raid team and additional key people should be trained to ensure they:

1) Understand the objective of a dawn raid.

2) Are aware of the authority's rights and process.

3) Understand the penalties involved in non-compliance.

4) Are prepared to handle the raid as it unfolds and know their roles and responsibilities during a dawn raid.

5) Understand how to ask and answer questions and provide information.

6) Anticipate the steps to be taken after the raid is completed, including the various teams to be involved, as outlined below.

b) In particular, relevant persons should be trained to:

1) Ask for a copy of the search warrant or authorizing instrument.

2) Ask authorities to wait for in-house or outside counsel.

3) Provide a room for the government to wait comfortably (such meeting rooms should be predesignated, adequately sized, and out of view, with access to restrooms; a separate meeting room for the organization's dawn raid team should be in proximity).

4) Be calm and friendly. Do not volunteer information.

5) Understand that, *consistent with local law*, it is their individual choice whether or not to give a statement to the government agents; that they have a right to have counsel present for any interview; that they may also decline to make any statement; and if they make a statement, it must be truthful.

6) Be aware that privacy and other data protection laws apply, including as to home inspections.

7) Avoid giving passwords without consultation with organization counsel.

8) Avoid giving unsupervised access to systems, and protest if demanded, unless otherwise directed by in-house or outside counsel.

9) Keep notes and document important aspects during the dawn raid, such as questions asked and documents inspected and taken.

10) Take reasonable steps to ensure material questions, requests, objections, and protests are recorded in the investigative minutes and contemporaneously in organization minutes.

c) The dawn raid team and additional key people should practice and be trained with mock exercises.

5. Safety and Security

a) In certain jurisdictions, inspectors or respective police support may be carrying firearms. The dawn raid team should make a positive determination of whether entrants will be armed, take this additional hazard into consideration, and warn organization personnel if appropriate.

b) If firearms or other weapons are on the premises, the inspectors should be alerted to the type of weapons and their location.

c) Organizations may be responsible for any unauthorized persons on the premises. Confirm the credentials and authorizing documentation of any persons seeking access under assertion of a dawn raid.

6. Data

a) Prepare a data map in advance that identifies and enables understanding of what sort of data is stored, where, and how. The data map may include information on typical data sources that will be requested during a dawn raid and how to preserve and collect it. It may be helpful to make use of existing electronic discovery procedures and tools. This will help in identifying and strategizing about the proper handling of protected, privileged, and sensitive information; in enabling the organization's response to any dawn raid (including minimization of data acquisitions and targeted data acquisitions by authorities); and in

helping to understand the organization's exposure from seized information and equipment.

b) Include employee personal/mobile devices and repositories in the assessment and indicate how employees maintain information of the organization. Mobile devices are fair game for seizure in many raids.

c) Identify access points for restricted information, including information maintained outside of the jurisdiction.

7. Technology Support

a) A forensic or electronic discovery technology and services consultant should be identified in advance to help assist with the response to a dawn raid and should possess the necessary equipment to cooperate and protect the organization's interests (e.g., sufficient hard drives to make two copies of whatever data the inspectors copy from organization repositories, without delaying government access).

b) Such a service may also be relevant for immediate analysis and review of seized data to deal with the legal follow-up.

8. Evidence Protection

a) If possible, copies should be made of everything seized, and the organization should make every effort to ensure that original documents are not taken from the premises.

b) Inspectors may, however, take materials without affording the opportunity for copying. To the extent possible, responsible persons should record how information was inspected and taken, what was taken, and obtain copies through post-inspection processes. Log files of searches on accessible systems should be secured.

    1) For instance, U.S. federal law enforcement typically will schedule time at a later date when counsel for the organization can come into the federal building with a copier and make copies of certain critical files or files otherwise afforded access.

c) Reasonable efforts should be made to identify sensitive materials, including personal information, trade secrets, and confidential information, and make this known to the government regulators.

d) If what is searched and taken is excessive, a qualified person (generally counsel) should lodge a protest and request that the authorities preserve but not review until a court can hear the issue.

9. Documentation and Debriefing

a) Once the search is complete, government investigators are required to leave a copy of the search warrant or the document authorizing the raid, along with a receipt of items seized. The receipt should provide a reasonably detailed description of data, documents, and other materials seized by the investigators.

b) Separately, the organization should prepare its own inventory of data, documents, and materials seized, and ask the government investigators to sign it, indicating what they have taken and what they agreed or did not agree to do. Although the government may decline to sign the organization's inventory, if done properly, it will be a critical contemporaneous record of the search and seizure.

c) The organization should hold a debriefing meeting with all members of the dawn raid team and conduct a postmortem of the raid in order to get a firm understanding of all actions that occurred, especially where in the facilities the inspectors went, who was interviewed, and what was accessed and copied or seized.

d) In-house or outside counsel should prepare a report of the raid, consolidating all notes taken by the dawn raid team, including all property and information taken, all information copied, all persons interviewed, all questions asked by investigators as well as answers given, and the authorizing documentation.

e) To the extent possible, identify and correct any inaccurate information provided to investigators.

f) The organization should follow up on unanswered questions or incomplete answers.

g) Management and employees should be instructed not to speak to the news media and to refer media inquiries to the designated contact.

h) Depending on the authorizing instrument, once government investigators have completed the raid and leave the premises, they are not allowed back, absent exigent circumstances, unless they obtain consent or obtain a new search warrant.

However, should the raid not be completed in one day, and the inspectors/agents indicate that the search will continue into another day, inspectors may return and seize additional evidence, including data, and may even seal the relevant portion of the premises pending completion.

Management and employees should be made aware and instructed accordingly.

i) The fact that a dawn raid has occurred at the organization's premises will likely become public knowledge through media reports. The organization should consider immediately preparing a press statement, which would be made available in response to media inquiries. The statement should be reviewed and approved by counsel for the organization before issuance.

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

Author: The Sedona Conference

Drafting Team Leader and Editor-in Chief
Maura R. Grossman

Senior Drafting Team Members and Executive Editors
Carolyn Anger
Gretel Best
Xavier Diokno
Lauren Fishman
Chuck Rothman

Drafting Members and Contributors
Kemi Atawo
Maite Bertaud
Colin Campbell
Angela Ellison
Emily Jennings
Michael Kasprowicz
Tatiana K. Lazadins
Matthew Maslow
David Meadows
Linda Misbah
Breanna Needham

Steering Committee Liaisons
Gretel Best
Lauren Fishman
Maura R. Grossman

Staff Editor: Craig Morgan

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, *The Sedona Canada Primer on Artificial Intelligence and the Practice of Law*, 26 SEDONA CONF. J. 99 (2025).

PREFACE

Welcome to The Sedona Canada *Primer* on Artificial Intelligence and the Practice of Law, a project of The Sedona Conference Working Group 7, "Sedona Canada" (WG7). This is one of a series of Working Group commentaries published by The Sedona Conference, a nonprofit, nonpartisan research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, data security, privacy, and artificial intelligence and the law

The mission of The Sedona Conference is to move the law forward in a reasoned and just way. The mission of WG7, formed in 2006, is "create forward-looking principles and best practice recommendations for lawyers, courts, businesses, and others who regularly confront e-discovery issues in Canada." Since The Sedona Canada Principles was released in early 2008 and was recognized by federal and provincial courts as an authoritative source of guidance for Canadian practitioners, WG7 has expanded its scope to address other issues in the law emerging from advances in technology. WG7's membership includes practicing attorneys, judges, government officials, technologists, academics, and legal service providers.

The WG7 Brainstorming Group on AI was formed in November 2022, the same month that the Generative AI boom was launched with the introduction of ChatGPT. A working outline was produced by May 2023. The initial draft underwent several revisions through 2024, as the technology evolved faster than the writing. Working drafts were presented at two public conferences on AI and the Law during 2024, and at the inaugural meeting of The Sedona Conference Working Group 13 on AI and the Law in January 2025. The drafting team considered comments and suggestions from members of both WG7 and WG13 in finalizing this *Primer*, with the full knowledge that by the time it is published, further advances in AI technology will

likely give rise to still more legal issues, which will need to be addressed in a later edition of the Primer or more focused commentaries that delve deeper into specific issues. In other words, this is very much a work-in-progress.

This *Primer* represents the collective efforts of many individual contributors at different stages of its development. In departure from our usual practice, we welcomed contributions from individuals who were not members of the Working Group Series to make sure all viewpoints and backgrounds were represented. For that reason, the acknowledgements on the masthead page are longer than usual, but the thanks are equally heartfelt. A special thanks, however, is due to Drafting Team Leader and Editor-in-Chief, Prof. Maura R. Grossman of the School of Computer Science at the University of Waterloo in Ontario, who persevered through 30 months from project conception to Primer publication. Thanks are also due to two usually unsung heroes, the volunteer research assistants who tracked down footnotes, checked citations, and guaranteed that there were no hallucinations, Angela Ellison and Jasmine Yu.

I should note that the *Primer*, like all Working Group Series publications, represents a high-level consensus of the writers, editors, contributors, and commentators, and does not necessarily reflect the individual views of the participants, their organizations, or their clients.

We encourage your active engagement in the ongoing dialogue addressing the legal issues raised by Artificial Intelligence. You can send comments and suggestions to comments@sedonaconference.org. If you are able to be more actively engaged, membership in The Sedona Conference Working Group Series is open to all. The Series includes WG7, WG13 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection law, international data transfers, data security

and privacy liability, 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.

Kenneth J. Withers
Executive Director
The Sedona Conference
June 2025

TABLE OF CONTENTS

I. INTRODUCTION

Artificial Intelligence ("AI"), a term that for most people existed primarily in the realm of science fiction, has swiftly transitioned into a pervasive reality in many sectors, including the legal domain.[1]The implementation of AI is reshaping the traditional contours of the legal profession, offering myriad opportunities while simultaneously presenting novel challenges.[2] This primer aims to provide a broad understanding of the role AI plays in the practice of law and its potential impact moving forward.[3]

AI refers to a collection of technologies that emulate human intelligence by performing cognitive tasks, e.g., perceiving, learning, reasoning, problem solving, and understanding and generating language.[4] Its application in law, while still in the relatively early stages, has already begun to influence various

1. Marcio Dpaulla, *Demystifying AI: A Comprehensive Guide for the Public*, LINKEDIN, (May 12, 2023), https://www.linkedin.com/pulse/demystifying-ai-comprehensive-guide-public-marcio-dpaulla.

2. Elijah Hartman, *How AI is Revolutionizing the Practice of Law*, HARRIS SLIWOSKI LLP BLOG, (Apr. 3, 2024), https://harris-sliwoski.com/blog/how-ai-is-revolutionizing-the-practice-of-law/.

3. Jeffrey M. Allen & Ashley Hallene, *AI Column: A Primer on Artificial Intelligence*, VOICE OF EXPERIENCE: January 2024 of the American Bar Association (Jan. 31, 2024), https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2024-january/primer-on-artificial-intelligence/.

4. Arun Rai et al. eds., *Next-Generation Digital Platforms: Toward Human-AI Hybrids*, 43 MIS QUARTERLY 3, 8 (2019), https://static1.squarespace.com/static/57d860b2ff7c5058ba601cb7/t/5e068e231b797629a15c0bca/1577487909476/EdComments_V43_I1+Next+Generation+Platforms+Human-AI+Hybrids+March+2019.pdf.

aspects of legal practice, from document review and legal research to contract analysis and prediction of legal outcomes.[5]

By way of example, in the realm of document review, AI can quickly sift through vast quantities of information, identifying and highlighting key pieces of evidence, thereby saving considerable amounts of time and money over purely manual processes. Legal research, a fundamental aspect of legal practice, appears to be on the cusp of a significant transformation, with new AI- and machine-learning driven systems enabling easy retrieval of targeted and relevant case law, statutes, and secondary sources in a matter of seconds, in response to a natural language query; a task that in the past might have taken hours, if not days of searching. AI's use in contract analysis has revolutionized the way that lawyers review and draft contracts. AI tools can identify standard clauses, flag missing clauses, and even suggest language based on the lawyer's past preferences, thereby increasing efficiency, and minimizing human error.[6] Finally, using machine learning algorithms, AI can analyze past judgments and rulings to forecast the possible outcome of a case, thereby assisting lawyers in formulating legal strategies.[7]

While these advancements offer immense potential, they also raise a host of ethical and practical challenges. As AI begins to automate aspects of the legal process, questions arise about

5. DRI Center for Law and Public Policy Artificial Intelligence Working Group, *Artificial Intelligence in Legal Practice: Benefits, Considerations, and Best Practices*, 18 DEFENSE RESEARCH INSTITUTE, (2024), https://www.dri.org/docs/default-source/dri-white-papers-and-reports/ai-legal-practice.pdf.

6. Andrea Carvajal, *Efficient Contracts: How AI is Revolutionizing Contract Drafting*, TOP LEGAL, (Jun. 13, 2023), https://www.top.legal/en/knowledge/ai-contract-drafting.

7. Jorge Argota, *Artificial Intelligence: The Game-Changer in the Legal Profession*, LINKEDIN, (Jul. 22, 2023), https://www.linkedin.com/pulse/artificial-intelligence-game-changer-legal-profession-jorge-argota.

the future role of human lawyers. There are concerns about data privacy and confidentiality, given the large volumes of sensitive information that AI systems handle. Additionally, the use of AI in the legal profession raises questions about bias and fairness, as these predictions are based on past decisions or other data, which may have been influenced by inherent biases.[8]

This *Primer* delves into these issues, providing an overview of how AI is transforming the practice of law. It aims to explore various types of AI tools currently in use, their implications for lawyers, law firms, clients, and judges, and potential future developments in this field. This *Primer* also discusses ethical considerations that arise from the use of AI in law and how the legal profession can navigate these challenges.

In essence, the intersection of AI and law presents a profound paradigm shift in the way legal services are and will be delivered. Whether one views this as a threat to the traditional legal profession, or an opportunity for growth and innovation, the fact remains that AI's impact on the practice of law will be massive and far-reaching. This *Primer* seeks to shed light on this evolving landscape, offering insights for legal practitioners, judges, law students, and anyone else interested in the future of legal services.

A. Scope

The focus of this paper is on AI systems that are designed to perform or automate a specific task and operate under a limited set of constraints. Present-day AI systems do not possess the

8. Jake Silberg & James Manyika, *Notes From the AI Frontier: Tackling Bias in AI (And in Humans)*, MCKINSEY GLOBAL INSTITUTE, (Jun. 6, 2019), https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/tackling%20bias%20in%20artificial%20intelligence%20and%20in%20humans/mgi-tackling-bias-in-ai-june-2019.pdf.

ability to understand, learn, or apply knowledge beyond the specific task for which it has been designed.

Some of the AI systems that are discussed in this paper include:

- *Predictive AI* which uses existing data to forecast future outcomes
- *Generative AI* that creates new content like text or images based on learned patterns
- *Discriminative AI* that focuses on classifying or categorizing existing data

Examples of such systems are prevalent in our everyday lives. These include Siri and Alexa, which use voice recognition to respond to user commands, large language models ("LLMs"), such as ChatGPT that use text and image prompts to respond in plain language, recommendation systems on e-commerce sites such as Amazon, which suggest products based on a user's browsing history, and AI in video games that adapt to a player's behavior.[9]

While present-day AI can mimic human intelligence for specific tasks, it does not possess true understanding or consciousness. It operates based on pre-programmed instructions or learned patterns and does not have the ability to tackle tasks outside its designed scope. Despite its limitations, this form of AI has made significant progress in numerous fields, including healthcare, finance, transportation, and entertainment.[10]

This paper does not encompass hypothetical future Artificial General Intelligence ("AGI") systems. AGI refers to a type of AI

9. Eban Escott, *What are the 3 Types of AI? A Guide to Narrow, General, and Super Artificial Intelligence*, CODEBOTS, (Oct. 24, 2017), https://codebots.com/artificial-intelligence/the-3-types-of-ai-is-the-third-even-possible.

10. Abid Ali Awan, *What is Narrow AI?* DATACAMP, (Jun. 28, 2023), https://www.datacamp.com/blog/what-is-narrow-ai.

that can learn, adapt, and solve an unlimited range of problems in a manner akin to a human being.[11] Unlike present-day AI which is designed to perform a specific task, AGI could potentially perform any intellectual task that a human being could—but it remains a theoretical concept subject to considerable debate.[12] Similarly, this primer will not cover "Superintelligence," which refers to an intellect that is significantly more advanced and capable than the human mind. It encompasses superior problem-solving skills, creativity, and knowledge in a wide spectrum of fields, such as scientific reasoning, social skills, and general wisdom.[13]

General AI and Superintelligence are briefly addressed in Section VII.

B. Automation vs. Augmentation

Automation and augmentation, although closely related concepts, have distinct implications, particularly in the context of AI and its applications.[14]

Automation refers to the process of using machines, robotics, or AI to perform tasks that were previously performed by humans, with minimal or no human intervention. It aims to increase efficiency, speed, and accuracy, and is often used for repetitive, routine tasks. Examples of automation include

---

11. *What is Strong AI*, IBM, (Oct. 13, 2021), https://www.ibm.com/topics/strong-ai#:~:text=If%20researchers%20are%20able%20to,indistinguishable%20from%20the%20human%20mind.

12. *See supra* note 11.

13. *Id*.

14. T. Emory, W. Louis, A. Poeppelmeier, K. Burns, "Automation in Legal Departments," Legal Operations in the Age of Al and Data, edited by O. Mack, H. Noorestani, and M. Onwudiwe, Globe Law and Business, January 2024, Chapter 1.

assembly lines in manufacturing plants, self-checkout systems in supermarkets, or email spam filters.

On the other hand, augmentation refers to the use of technology to enhance or improve human capabilities, rather than to replace them. Augmentation tools are designed to assist humans in performing tasks more effectively and efficiently by providing insights, decision-making support, or enhanced abilities. Examples of augmentation include AI-driven document-review analysis tools that enhance lawyers' ability to make decisions about sets of documents, or Global Positioning Systems ("GPS") that enhance our natural navigation abilities.[15]

In essence, while automation aims to replace human effort, augmentation aims to enhance it. Both have significant roles to play in the future of legal work and the legal profession, and the balance between them is a key consideration in the design and implementation of AI systems.

15. Nexlogica Team, *AI in IT: From Automation to Augmentation*, NEXLOGICA, (Aug. 30, 2023), https://www.nexlogica.com/ai-in-it-from-automation-to-augmentation/.

II. TYPES OF ARTIFICIAL INTELLIGENCE AND THEIR APPLICATIONS

A. Expert Systems

An Expert System is a computer system that emulates the decision-making ability of a human expert using AI techniques. Expert systems are designed to solve complex problems by applying dynamically created logical rules rather than through conventional procedural code. Expert systems were among the first truly successful applications of AI, with the first systems appearing in the late 1970s.[16]

An expert system is divided into two subsystems: the inference engine and the knowledge base. The inference engine subsystem applies rules to known facts to deduce new facts. Inference engines can also include explanation and debugging abilities.[17]

Originally, the knowledge base subsystem was composed of pre-defined facts and rules. With the advent of machine learning, big data, and data-mining techniques, modern expert systems can now incorporate new knowledge more easily and thus readily update themselves. Such systems can generalize from existing knowledge to better deal with vast amounts of complex data.

B. Machine Learning

Machine Learning is used for solving problems where developing algorithms (i.e., sets of rules to accomplish a goal) by human programmers could be too expensive or time-consuming.

---

16. PETER JACKSON, INTRODUCTION TO EXPERT SYSTEMS 2 (3d ed., 1998).

17. V. DANIEL HUNT, ARTIFICIAL INTELLIGENCE & EXPERT SYSTEMS SOURCEBOOK (1986), *available at* https://link.springer.com/book/10.1007/978-1-4613-2261-0.

Machine-learning systems solve problems by having the computer system build a model of the problem without needing to be explicitly instructed what to do, step by step, by human-developed algorithms. In other words, machine learning systems infer the rules necessary to accomplish a task without specifically having been programmed with those rules.

Machine-learning approaches have been applied to computer vision, speech recognition, email filtering, legal document review, agriculture production, and medical research and diagnosis, and other areas.[18]

Machine-learning approaches can be divided into several broad strategies or implementations, including:

- Unsupervised Learning
- Supervised Learning
- Reinforcement Learning
- Deep Learning[19]

Unsupervised Learning takes a set of data and looks for some type of structure, like groupings or clustering of data points. Instead of responding to human feedback, as is the case with supervised learning, unsupervised learning autonomously identifies commonalities and/or anomalies in the data to build its model. An example of unsupervised learning is document clustering where documents with similar topics or traits are grouped together.

---

18. Oludare Isaac Abiodun et al., *State-Of-The-Art in Artificial Neural Network Applications: A Survey*, 4 HELIYON, (Nov. 23, 2018), https://www.sciencedirect.com/science/article/pii/S2405844018332067.

19. Iqbal H. Sarker, *Machine Learning: Algorithms, Real-World Applications and Research Directions*, 2 SN COMPUT. SCI. 160, (2021), https://link.springer.com/article/10.1007/s42979-021-00592-x.

Supervised Learning builds a mathematical model from a set of labeled training data (i.e., positive and negative exemplars), typically through an iterative approach of labeling the data and testing it by having humans also apply categorization labels.[20] For example, the training data set could be a set of documents to be reviewed by a producing party in litigation. An active supervised learning system would present a small subset of the documents to human lawyers and ask them to indicate if the contents of the document are responsive or unresponsive to the requesting party's Requests for Production. The system would then use the contents of the documents and the human coding decisions to build a decision model. It would then continue to present subsets of the documents to the lawyer for coding, updating the model with each iteration. When the model's decisions and the lawyer's decisions match, the model is said to have stabilized and can be relied upon to categorize the remaining documents.[21] This process has typically been referred to as "TAR 1.0."[22]

Reinforcement Learning involves a software agent that senses a situation, takes actions, and receives a reward signal indicating positive or negative outcomes.[23] The algorithm learns over time how to maximize the total reward value it receives. Examples of reinforcement learning algorithms are those used in

---

20. *Id*.

21. Heather Heavin & Micheala Keet, CIAJ 2016 Annual Conference "Civil Justice and Economics: A Matter of Value", *The Path of Lawyers: Enhancing Predictive Ability Through Risk Assessment Methods*, (Oct. 5-7, 2016), https://ciaj-icaj.ca/wp-content/uploads/2016/11/930.pdf.

22. Rachel McAdams, *A Crash Course in TAR: What Do You Really Need to Know?* INTERNATIONAL LEGAL TECHNOLOGY ASSOCIATION, (Jan. 24, 2022), https://www.iltanet.org/blogs/rachel-mcadams1/2022/01/24/a-crash-course-in-tar-what-do-you-really-need-to-k.

23. *Reinforcement Learning*, GEEKS FOR GEEKS, (Feb 24, 2025), https://www.geeksforgeeks.org/what-is-reinforcement-learning/.

autonomous vehicles, or in systems used to play a game against a human opponent.

Deep Learning involves a series of layered algorithms, starting with an input layer, followed by hidden layers, and then an output layer. Each layer performs a different function and passes certain information on to the next layer. Often referred to as a neural network because the logical structure and functioning is akin to a biological brain, with interconnected nodes and synapses, deep learning enables machines to perform complex tasks and make accurate decisions without help from humans. Deep learning systems can be far more capable for certain tasks than other machine-learning models. Like supervised and reinforcement learning, deep learning requires training to ensure accurate results. Examples of deep learning include computer vision (e.g., interpreting and labeling images) and generative AI (e.g., developing new creations based on existing data).

C. Applications

1. AI-Generated Images

Computer graphics is a field of computer science in which computers apply various algorithmic and mathematical processes to create or manipulate images. Computer graphics is applied in many areas, including video games, animated films, visual effects, computer-aided design ("CAD" drawings), computer-aided manufacturing ("CAM"), simulations, medical imaging, and information or data visualization.[24]

Recent advances in AI allow computers to generate images based on the text submitted by a user (e.g., a cute white kitten dreaming of goldfish). These text-to-image applications are a form of Generative Artificial Intelligence ("Gen AI"), whereby a

24. Steve Marschner & Peter Shirley, FUNDAMENTALS OF COMPUTER GRAPHICS 1-3 (5th ed., 2015).

computer can generate new content such as text, audio, images, or video. A Diffusion Model is a form of Gen AI model that can generate new images that are similar to those on which the model was trained. By adding random noise to the trained images, the model learns how to remove the noise and to construct the image described by the user.[25]

2. Computer Vision

Computer vision is another area of computer science that deals with images and videos. Unlike computer graphics, where computers create or manipulate images and videos, computer vision uses computers to identify objects and people within those media. Generally, a computer vision application analyzes an image or video in three steps. First, a sensor device, such as a camera or medical imaging device, captures the image. Next, the image is passed to an interpreting device that breaks down the image into patterns and compares those patterns against the library of patterns on which the application has been trained. Finally, a user submits a request about the image (e.g., is the person in the image a company employee?) and the interpreting device provides an answer from its pattern analysis.[26]

Computer vision and AI are applied in developing autonomous driving vehicles. For example, Google's Waymo vehicles come with an array of sensors that collect data from the surrounding world. The onboard computer uses deep learning to train on the sensor data. This training enables the computer to predict things before they occur by gathering real-time data

25. Victor Dey, *How Diffusion Models Unlock New Possibilities for Generative Creativity*, VENTUREBEAT, (Oct. 26, 2022), https://venturebeat.com/ai/how-diffusion-models-unlock-new-possibilities-for-generative-creativity.

26. *What is Computer Vision?* MICROSOFT AZURE RESOURCES, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-computer-vision (last visited Feb. 19, 2025).

mixed with its experience of real-world driving, and plan for safe outcomes by quickly determining trajectory, lane, speed and steering maneuvers. [27]

In addition to identifying objects, computer vision and AI is also used for searching and classifying images. For example, Amazon's Rekognition is an image-recognition service that detects objects, scenes, activities, landmarks, faces, dominant colors, and image quality. When searching for faces, Rekognition applies deep learning to identify faces within an image. When a face is identified, the application applies a rectangular frame around the face along with a confidence score indicating the likelihood of the match.[28]

3. Speech Recognition

Speech-recognition programs process human speech into a written format. These programs are often referred to as automatic speech recognition ("ASR"), computer speech recognition, or speech-to-text. Speech recognition is used across many industries, including automotive, technology, legal, healthcare, sales, and security. Typically, these applications consist of several components, such as speech input (e.g., an audio recording or a user's voice), feature extraction, feature vectors, a decoder, and the text output.[29]

For example, transcription services are commonly used in the legal industry and allow lawyers to take a recording (e.g., of a deposition or client interview) and upload the recording to a

27. Mallika Rangaiah, *How Waymo is using AI for autonomous driving?* ANALYTICS STEPS, (Jul. 15, 2021), https://www.analyticssteps.com/blogs/how-waymo-using-ai-autonomous-driving.

28. *What is Amazon Rekognition Image?* AMAZON WEB SERVICES, https://aws.amazon.com/rekognition/image-features (last visited Feb. 19, 2025).

29. *What is Speech Recognition?* IBM, (Sep. 28, 2021), https://www.ibm.com/topics/speech-recognition (last visited Sep. 20, 2024).

transcript service site. The lawyer can then download a computer-generated transcript that can be at least 90% accurate.[30] Speech recognition programs also apply AI, allowing the program to learn and improve transcription accuracy as more speech is processed. These programs may use neural networks to analyze and train on various aspects of language, such as grammar, syntax, and structure.[31]

4. Audio Search

In eDiscovery, speech recognition programs are also used to search voicemails or call centre recordings. Once these recordings are converted to a transcript, search and analytics tools can be used to identify relevant portions of the recording. For example, Intelligent Voice is a tool that is available within Relativity's eDiscovery application. This tool allows a user to interact with an audio player that plays the audio file alongside the text transcription. The user can search the transcript, review a summary of main topics discussed, and jump to various parts of the conversation.[32]

5. Audio Generation

In addition to converting human speech into text, computer applications can convert text to audio, such as human speech, music, and ambient environmental sounds. Text to speech ("TTS") or speech synthesis technology are used in virtual assistants, where a computer generates the virtual assistant's

30. *How to Automatically Transcribe Your Audio and Video to Text*, REV, https://www.rev.com/blog/resources/how-to-automatically-transcribe-audio (last visited Feb. 19, 2025).

31. *See supra* note 27.

32. *Intelligent Voice for Audio and Video Discovery in Relativity*, RELATIVITY, https://www.relativity.com/relativity/assets/pdf/Intelligent-Voice-Audio-Video-Discovery-in-Relativity.pdf (last visited Feb. 19, 2025).

synthetic voice based on written text. These virtual assistants humanize the transaction and assist visually impaired users as well as those who are vocally challenged.

To generate a human-like voice, TTS applications primarily perform text and linguistic analysis to generate an audio waveform. During the text analysis, the text is analyzed and converted into full words and sentences. Any abbreviations are expanded, and expressions are identified. Linguistic analysis is then performed to understand the grammatical structure and to refine the synthetic voice's pitch and duration. The results are used to produce a spectrogram (a visual representation of the sound over a period of time) that is later converted into human-like speech.[33]

III. HOW ARTIFICIAL INTELLIGENCE IS USED IN LEGAL PRACTICE

A. eDiscovery

1. Word Clustering

Clustering is a form of unsupervised machine learning. It analyses the eligible documents in a collection (those with sentences) and builds an index of concepts based on the words used in the sentences. Once the index is created, it can be used to search for documents that discuss similar topics. It can also group documents containing similar concepts into clusters.

Conceptual clusters can be used to quickly gain a better understanding of the makeup of a collection of documents and make broad coding decisions such as denoting specific clusters as potentially responsive, or potentially not responsive. Such determinations should be confirmed through quality control.

---

33. Mikiko Bazeley, *An Easy Introduction to Speech AI*, NVIDIA DEVELOPER, (Jun. 23, 2022), https://developer.nvidia.com/blog/an-easy-introduction-to-speech-ai.

2. Technology-Assisted Review ("TAR")

AI has been used in eDiscovery for more than a decade to search, classify, and code documents during the review process. This is commonly referred to as Technology-Assisted Review ("TAR"). TAR, in all its forms, uses either supervised machine learning and/or natural language processing ("NLP") to analyze textual content. NLP is the field of computer science that enables computers to understand, interpret, and generate human language.[34] It involves several tasks such as machine translation, speech recognition, sentiment analysis, and topic segmentation.[35] This means that TAR techniques can only be applied to certain types of records—those that contain sufficient textual content—such as emails, letters, contracts, and some spreadsheets, but usually not images. There are generally two types of TAR: TAR 1.0 (Simple Active Learning) and TAR 2.0 (Continuous Active Learning).[36]

Both TAR 1.0 and TAR 2.0 rely on supervised machine learning, with human subject matter experts ("SMEs") training the model to identify responsive and non-responsive documents. The classifications made by the human SMEs on a subset of documents are used to build a model that can then be applied to all

34. Grady Andersen & MoldStud Research Team, *The Role of Natural Language Processing in Computer Science* (Feb. 12, 2024), MOLDSTUD, https://moldstud.com/articles/p-the-role-of-natural-language-processing-in-computer-science.

35. *Natural Language Processing*, HYPERSCIENCE, https://www.hyperscience.com/knowledge-base/natural-language-processing/ (last visited Feb. 19, 2025).

36. Maura R. Grossman & Gordon V. Cormack, *Technology-Assisted Review in Electronic Discovery*, DATA ANALYSIS IN LAW, (Ed Walters ed., 2018), https://www.iadclaw.org/assets/1/7/10.2-_Grossman_and_Cormack_-_TAR_in_Electronic_Discovery.pdf.

documents in the collection, categorizing or ranking them by their responsiveness.

In a TAR 1.0 workflow, there is a fixed training set. Once stabilization is reached (i.e., the point at which it is determined that the model will no longer improve with a proportionate amount of effort), training is stopped and the model is used to separate the documents into presumptively responsive and presumptively non-responsive documents. In a TAR 2.0 workflow there is no fixed training set. Documents continue to be reviewed and fed back into the model for further training until the number of responsive documents being found no longer justifies the effort necessary to find them. This notion is referred to as marginal precision.[37]

TAR is most often used to expedite determinations of relevance, both in reviewing documents to be produced, and in reviewing documents that were produced by the other side. Practitioners typically use TAR to prioritize records for review, allowing them to avoid reviewing documents unlikely to be relevant. TAR can also be used to classify relevant or responsive documents into specific issues, using the same techniques as those used to identify relevance. With proper quality controls, TAR can also be used for privilege determinations, although work product can be challenging to identify with machine learning it is advisable for TAR to be applied in conjunction with other methods, including search terms, when it is used for privilege review. Regardless of the purpose for using TAR, quality control measures, such as sampling of the unreviewed

37. Gordon V. Cormack & Maura R. Grossman, *Multi-Faceted Recall of Continuous Active Learning for Technology-Assisted Review*, SIGIR '15: Proc. of the 38th Int'l ACM SIGIR Conf. on Res., & Dev. In IR, 763, 765 (2015), https://dl.acm.org/doi/pdf/10.1145/2766462.2767771.

documents,[38] are necessary to ensure the defensibility of the review process.

Clustering and TAR are not mutually exclusive; many review workflows use both unsupervised and supervised TAR techniques together to achieve more efficient results.

B. Identification and Redaction of Personally Identifying Information and Personal Health Information

AI technologies can be used to automatically identify personal information, including Personally Identifying Information (PII) and Personal Health Information ("PHI"). This can be particularly useful when documents are produced in litigation or regulatory matters, to comply with privacy regulations, and when responding to a data breach.

PII and PHI detection is facilitated by a collection of AI and machine-learning algorithms that perform entity extraction, an information extraction technique that identifies key elements from text and classifies it into predefined categories. Different methods of detection may be used, including pattern matching, NLP, and LLMs.[39]

C. Sentiment Analysis

Sentiment analysis uses NLP to analyze the content of text and speech, and to categorize the emotional tone of that content, such as positive, negative, or neutral. This technique is particularly useful in cases involving sexual harassment, workplace

---

38. *Project Validation and Elusion Testing*, RELATIVITY ONE, https://help.relativity.com/Server2023/Content/Relativity/Active_Learning/Elusion_Test.htm (last visited Feb. 19, 2025).

39. Arun Narayanan, *From Data Deluge to Discovery: Navigating E-Discovery Challenges with Generative AI*, HEXAWARE, (Jun. 5, 2024), https://hexaware.com/blogs/from-data-deluge-to-discovery-navigating-e-discovery-challenges-with-generative-ai/.

investigations, and insider trading investigations, where records that are particularly positive or negative in tone can quickly be identified and prioritized for review.[40]

Sentiment analysis is also a valuable business intelligence tool that provides organizations with external and back-office insight allowing them to triage and improve customer service requests and responses, monitor brand sentiment, conduct market research through social media and online sources, and track marketing campaign performance. Internally, organizations can use sentiment analysis to gauge employee engagement and satisfaction and to gain insight into employee responses to workflow and process improvements and business initiatives.[41]

D. Language Detection and Translation

Language detection and translation uses NLP or LLMs to analyze the content of text and speech to identify the primary and other languages used in those documents. AI translation services can translate text into many languages.[42]

In eDiscovery, language detection can be used to identify and categorize documents by language so that records containing a specific language can be directed to a reviewer fluent in that language. On-the-fly translation can be used so that reviewers who are not fluent in a particular language can translate the document and review it, funneling only those that need it for more expensive human translation.

---

40. *Natural Language Processing (NLP)*, PROOFPOINT, https://www.proofpoint.com/us/threat-reference/natural-language-processing (last visited Feb. 19, 2025).

41. Catherine Tansey, *How to Measure Employee Sentiment and Why It Matters*, EDEN, (Feb. 7, 2023), https://www.edenworkplace.com/blog/how-to-measure-employee-sentiment-and-why-it-matters.

42. Rafael Timbó, *NLP vs. LLM: Differences, Uses, and Impacts*, REVELO, (Dec. 31, 2024), https://www.revelo.com/blog/nlp-vs-llm.

Organizations can also use language detection and translation to improve user experience,[43] such as: translation of website or social media content to another language based on the source country location of the website or social media traffic; triaging foreign language customer service requests to specific representatives who can read and converse in that foreign language; and translation of foreign business documents.

E. Transforming Audio to Text

Audio-to-text conversion tools transcribe audible speech into text. Once transcribed, other techniques (such as clustering and TAR) can be applied to classify and review the information. While audio can be transformed to text manually or by using traditional transcription software, the use of AI for transcriptions has improved the speed, quality, and cost of audio-to-text conversions.[44]

Audio-to-text conversion tools are also available as standalone products, but some review software platforms incorporate additional features for audio-to-text conversion. For example, Intelligent Voice is a tool that is available within Relativity's eDiscovery application. This tool allows a user to interact with an audio player that plays the audio file alongside the text transcription. The user can search the transcript, review a

43. *Using Language Detection and Dynamic Machine Translation in Virtual Agent*, SERVICENOW, https://docs.servicenow.com/bundle/washingtondc-servicenow-platform/page/administer/virtual-agent/concept/dynamic-lang-detection-translation.html (last visited Feb. 19, 2025).

44. André Bastié, *Is Automatic Transcription a Good Practice for Qualitative Research Methodology?* HAPPYSCRIBE, (Oct. 31), https://www.happyscribe.com/blog/en/is-automatic-transcription-good-practice-for-qualitative-research-methodology (last visited Feb. 19, 2025).

summary of main topics discussed, and jump to various parts of the conversation.[45]

In the context of document review, selection of review software that can provide high-quality audio transcription within the review platform can streamline a workflow, resulting in cost efficiencies for the processing and review stages of an eDiscovery project.

F. Image Classification

Image classification is a process that employs AI to label properties within a visual image, such as a photograph, and assign labels to represent those properties. For example, a photograph may contain people, buildings, vehicles, groundwork, etc. The extent and specificity of the labelling is dependent on the specific implementation used. A single image will typically have several labels. Some implementations will include the confidence in the labelling (i.e., a measure of the AI system's confidence that the label is accurate).[46]

Once the labels have been created, they can be used to group images together for review and analysis. The labels can also be used to identify PII or PHI for regulatory requirements or for withholding or redacting prior to production. The labels can also be used for those with visual impairments to understand the content of documents they cannot see.

---

45. *Intelligent Voice for Audio and Video Discovery in Relativity*, RELATIVITY, https://www.relativity.com/relativity/assets/pdf/Intelligent-Voice-Audio-Video-Discovery-in-Relativity.pdf (last visited Feb. 19, 2025).

46. Jasper van der Waa, Tjeerd Schoonderwoerd, Jurriaan van Diggelen, and Mark Neerincx, et al., *Interpretable confidence measures Confidence Measures for decision support systems*, *Decision Support Systems*, 144 INTERNATIONAL JOURNAL OF HUMAN-COMPUTER STUDIES, Volume 144 (Dec. 2020), 102493, https://www.sciencedirect.com/science/article/pii/S1071581920300951 (last visited September 23, 2024).

Review and classification of images is a key aspect for analysis and review of data from mobile phones, other portable devices, chat-platform data, and social media accounts, which typically contain many images.[47]

G. Data Breach Response

AI can play a significant role in identifying PII during the reporting process in response to a data breach. This is particularly important because quick and accurate identification of the information that has been compromised is crucial for determining the appropriate response measures, including who needs to be notified and what regulatory filings may be required.[48]

AI entity identification can be used to identify the specific pieces of PII that were involved in the breach. This could include names, email addresses, social security numbers, financial information, or other sensitive data.[49] In addition, AI can be effective in linking named entities to people. This process involves training an AI model to understand and reconize specific categories of information, such as people's names, within a document. The system does this by learning from a large set of training data, which includes various types of documents where the named entities and their corresponding categories have been annotated. Over time, the AI model learns to identify patterns and

47. Ritu John, *What is Image Classification: Applications, Techniques & Tools for Enhanced Data Extraction*, DOCSUMO, (Nov. 15, 2024), https://www.docsumo.com/blogs/data-extraction/image-classification.

48. Thought Leadership, *How AI Improves PII Compliance & Data Privacy*, DFIN, (Oct. 10, 2023), https://www.dfinsolutions.com/knowledge-hub/thought-leadership/knowledge-resources/protecting-pii-with-ai-and-chatgpt.

49. Roman Vinogradov, *Understanding the Role of Personally Identifiable Information (PII) in Business*, IMPROVADO, (Feb. 13, 2025), https://improvado.io/blog/what-is-personally-identifiable-information-pii.

contexts that indicate a particular string of text is a named entity related to a person.[50]

For instance, the AI can be trained to recognize that Mr. John Doe or Dr. Jane Smith in a document likely refer to individuals. Furthermore, the AI can also learn to discern contextual clues to link named entities to specific people.[51] For example, if a document mentions that John Doe's birthday is June 1, 1981, the AI can determine that June 1, 1981 is a date, is personal information (a birth date), and is associated with John Doe (a person).

Moreover, AI can also perform co-reference resolution techniques to link different mentions of the same person within a document.[52] For example, if a document initially refers to President John Doe and later mentions "the President," the AI can infer that both may refer to the same individual.

Importantly, while AI can be a powerful tool in identifying PII and the associated individuals in response to a data breach, it is not infallible. Human oversight and expertise are still necessary to ensure accuracy and compliance with all relevant laws and regulations.[53]

---

50. Kalyani Pakhale, *Comprehensive Overview of Named Entity Recognition: Models, Domain-Specific Applications and Challenges*, INNOVER DIGITAL, (Sep. 25, 2023), https://arxiv.org/pdf/2309.14084.

51. AltexSoft Editorial Team, *Named Entity Recognition: The Mechanism, Methods, Use Cases, and Implementation Tips*, ALTEXSOFT, (Oct. 31, 2023), https://www.altexsoft.com/blog/named-entity-recognition/.

52. Marta Maślankowska & Paweł Mielniczuk, *Intro to Coreference Resolution in NLP*, NEUROSYS, (May 4, 2022), https://neurosys.com/blog/intro-to-co-reference-resolution-in-nlp.

53. Megha Thakkar, *AI Compliance: Meaning, Regulation, Challenges*, SCRUT AUTOMATION, (Jan. 21, 2025), https://www.scrut.io/post/ai-regulatory-compliance.

H. Information Governance

Recordkeeping practices evolve with the changes in society. AI technology has enabled records managers and information governance (IG) professionals to manage records systems more effectively.[54]

The first stage of any IG implementation is data classification. Without accurate and appropriate classifications, IG functions cannot work. Traditionally, classification was a manual process; a person, typically the record creator or a records manager, would review a record to determine its type (e.g., letter, memo, contract). Additional information such as its date, author and recipients, department or case, would also be classified.

AI-powered systems are now available to automatically classify records, using a combination of predefined taxonomies and machine-learning techniques to parse the information within a record and apply one or many classifications. These systems continuously improve their accuracy and efficiency through user interactions and feedback.[55]

With the help of AI, search engines can understand natural language queries and find relevant documents based on their content. AI can also enhance the searchability and organization of documents by extracting significant metadata such as dates, authors, titles, and keywords. This is especially beneficial when

54. James Lappin, *Records Management Before and After the AI Revolution*, THINKING RECORDS, (Jan. 30, 2020), https://thinkingrecords.co.uk/2020/01/30/records-management-before-and-after-the-ai-revolution/.

55. Victoria Sivaeva, *Knowledge Taxonomy AI that Organizes Information Automatocally*, MATRIXFLOWS, https://www.matrixflows.com/blog/ai-powered-taxonomies-for-knowledge-management (last visited Feb. 19, 2025).

dealing with large records databases, as manually searching for specific information can be time-consuming.[56]

AI can help with data governance and compliance, ensuring regulations like The Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's federal privacy law for private sector organizations, and Quebec's Law 25, the latest and most significant privacy legislative development in Canada, are followed.[57] AI can automate tasks related to data privacy, compliance, and security.[58]

I. Mergers and Acquisitions Due Diligence

AI has been integrated into several specialized due diligence review platforms. These systems use AI to identify and extract specific information, such as the parties to a lease, the location of the property at issue, and the term and price of the rental. They are also often used to identify and extract particular contract clauses, such as indemnity clauses, termination clauses, or non-compete clauses.[59] These systems can scan through large volumes of contracts and pull out the relevant sections for

---

56. Laurence Hart & Jonathan Bordoli, *How Automated Content Tagging Improves Findability*, TECHTARGET, (Oct. 19, 2020), https://www.techtarget.com/searchcontentmanagement/tip/AI-in-content-management-supports-tagging-search.

57. Shreya, *Quebec's Law 25: What You Need To Know*, COOKIEYES, (Jul. 16, 2024), https://www.cookieyes.com/blog/quebec-law-25/.

58. Canada PIPEDA, *Everything You Need To Know About Quebec's Law 25: A Comprehensive Guide to Privacy and Data Protection in Canada* [Updated 2024], SECURE PRIVACY, (Mar. 5, 2024), https://secureprivacy.ai/blog/quebec-law-25-guide-2024.

59. *Advanced Contract Analytics is Emerging with Game-Changing Insights*, IRONCLAD JOURNAL, https://ironcladapp.com/journal/contract-data/advanced-contract-analytics/#:~:text=AI%20models%20can%20be%20trained,comparing%20clauses%20across%20multiple%20contracts (last visited Feb. 19, 2025).

review. The AI is also used to identify areas of potential risk in contract clauses, such as overly broad indemnification clauses or unusual termination provisions. The system can flag these areas for further human review.

Such AI features can also compare clauses across multiple contracts to ensure consistency. They can identify deviations from an organization's standard language, which can be particularly helpful in large-scale contract reviews.[60]

J. Contract Analytics

With AI becoming the norm in many areas of legal practice, it is not surprising that contract analytics has become top of mind for corporate lawyers. Lawyers can use both discriminative AI[61] and Gen AI to quickly review and analyze contracts, thereby achieving efficiencies and cost savings for their clients.

Like due diligence tools, these tools use predictive AI to pre-train models to identify similar provisions in large contract repositories (e.g., post-execution review). The models are often trained on a large volume of common contractual clauses, which may reduce the amount of time required for human review of specific portions of a contract. In addition to pre-trained models, many of these tools allow users to train models on clauses or concepts that are not pre-trained, either because they are uncommon or bespoke. Using these training examples, the contract analytics tool can then identify similar clauses across a large volume of contracts. AI tools that permit users to train

60. Sebastian Wengryn, *How AI-Supported Document Analysis Simplifies Processes and Saves Time*, CONTRACTHERO, https://en.contracthero.com/blog/ki-gestuetzte-vertragsanalyse (last visited Feb. 19, 2025).

61. Kanerika Inc., *Generative Vs Discriminative: Understanding Machine Learning Models*, MEDIUM, (May 11, 2024), https://medium.com/@kanerika/generative-vs-discriminative-understanding-machine-learning-models-87e3d2b3b99f.

their own models are also generally language agnostic and can be trained in any language. Contract analysis tools may also be useful for identifying large groups of similar contracts, similar clauses and identifying anomalies or outliers.[62] In addition to discriminative AI, Gen AI technologies are now being used to automate and generate clause summaries.

In addition to post-execution review, emerging Gen AI technologies are now being used to facilitate the drafting and negotiation of contracts.[63] In addition to automatically generating contracts or contract clauses, as Gen AI tools mature, we are seeing increased ability for these tools to identify areas where a contract differs from specific agreed terms and identify provisions that are not in compliance with the pre-defined policies or rules for those types of agreements.

Users of these tools should be cautioned that the systems have limitations and risks associated with them, often depending on the quality of their training. Users should therefore take care to be fully informed of such limitations and risks. It will undoubtedly be critical for lawyers to adopt these technologies to remain competitive, but they should approach such new technologies with caution to ensure that they are acting ethically and responsibly.

K. Fraud Detection and Compliance

AI and machine-learning algorithms can analyze patterns and trends across massive databases of financial transactions.

---

62. Prajeesh Prathap, *Anomaly Detection With Variational Autoencoders (VAE): Unveiling Hidden Patterns*, MEDIUM, (Jul. 7, 2023), https://medium.com/@prajeeshprathap/anomaly-detection-with-variational-autoencoders-vae-unveiling-hidden-patterns-42631834ffbf.

63. Jay Ghatge, *AI Co-Pilots: Revolutionizing Contract Negotiation and Drafting*, SPEEDLEGAL (May 27, 2024), https://speedlegal.io/post/ai-co-pilots-revolutionizing-contract-negotiation-and-drafting.

They can identify unusual transactions or behaviours that could indicate fraud, such as sudden large withdrawals, repeated transactions within a short period of time, or transactions in high-risk locations.

AI can also be used to automate the process of checking transactions and customer behaviour against regulatory requirements. This includes monitoring for money laundering, confirming customer identities, and ensuring that all necessary information is collected and stored correctly. The risk associated with transactions, customers, or products can automatically be assessed by analyzing historical data, customer behaviour, and market trends to predict potential risks and suggest actions to mitigate such risks.

L. Legal Research

According to a study by the American Bar Association (ABA), the average lawyer spends between 16% and 25% of their time performing legal research.[64] AI has recently been incorporated into several commercial, online legal research platforms in an effort to make the process more streamlined, efficient, and accurate.[65]

Using NLP, legal research systems can learn the context and intent behind a user's search query, as opposed to merely matching specific words contained in both the search query and the results. This allows the search system to find responsive information that may contain words or phrases that are different from what the user entered, but which carry the same contextual

64. Steven A. Lastres, *Rebooting Legal Research in a Digital Age*, LLRX, (Aug. 10, 2013), http://www.lxisnexis.com/documents/pdf/20130806061418_large.pdf.

65. *What is AI and How Can Law Firms Use it?*, CLIO, https://www.clio.com/resources/ai-for-lawyers/lawyer-ai/ (last visited Feb. 19, 2025).

meaning.[66] A study carried out by the National Legal Research Group[67] found that using AI-enabled legal research tools made the process 24.5% more efficient, saving a lawyer between 132 and 200 hours of legal research time per year. The researchers also found that the search results were 21% more responsive than when using traditional, keyword-based search techniques.

M. Legal Drafting

Through machine learning and NLP, AI can potentially automate and streamline the legal drafting process, making it more efficient and comprehensible.[68]

Expert systems are AI structures based on a set of rules and heuristics, which emulate the decision-making ability of a human expert. In the context of legal document drafting, an expert system can be programmed with a set of rules related to the structure and content of specific legal documents. When provided with the necessary inputs, the system can generate a draft document following those rules.[69]

Predictive text technology can be used in applications to speed up the document-drafting process. The AI learns from previously written legal documents and suggests the next word

66. Pankaj Pandey, *Exploring Semantic Search Using Embeddings and Vector Databases With Some Popular Use Cases*, MEDIUM, (Aug. 10, 2023), https://medium.com/@pankaj_pandey/exploring-semantic-search-using-embeddings-and-vector-databases-with-some-popular-use-cases-2543a79d3ba6.

67. National Legal Research Group, *The real impact of using artificial intelligence in legal research*, LAWNEXT, (2018), https://www.lawnext.com/wp-content/uploads/2018/09/The-Real-Impact-of-Using-Artificial-Intelligence-in-Legal-Research-FINAL2.pdf (last visited September 23, 2024).

68. *AI Transforms Legal Workflows: Automation & Efficiency*, CIMPHONY, https://www.cimphony.ai/insights/ai-transforms-legal-workflows-automation-and-efficiency (last visited Feb. 19, 2025).

69. For example, leveraging existing playbooks for the drafting of simple, standard form contracts.

or phrase as the lawyer types. This can accelerate the drafting process and ensure the use of standard legal language. Similarly, this technology, when trained on a large corpus of legal documents, can suggest relevant clauses or sections to be included in a new document based on the type of document being drafted and the specific details of the case.

However, the most revolutionary use of AI as it pertains to legal document drafting involves Gen AI. Gen AI uses deep learning models and NLP to generate new content in response to a user prompt.[70] It can be used to automate the creation of legal documents such as motions, briefs, contracts, wills, and letters, and can also be used to review or customize existing documents. By learning from previous documents and the preferences of the user, the AI can suggest changes or additions to make the document more suited to the user's needs. This can include suggesting alternative phrasing for clauses, adding or removing clauses based on the specific situation, or even providing explanations for certain legal terminology in plain English.

Moreover, when used correctly, Gen AI can help in maintaining consistency across multiple documents. It can ensure that the same language and terminology are used across all documents, which can be particularly useful in large legal cases that involve numerous documents.

However, while Gen AI can greatly enhance the efficiency of drafting legal documents, it is crucial to note that it cannot replace the oversight and expertise of a legal professional. Lawyers must review the AI-generated output to ensure its accuracy and compliance with all relevant laws and regulations, particularly in light of the fact that Gen AI is prone to hallucinations or

70. Cole Stryker & Mark Scapicchio, *What is Generative AI?* IBM, (Mar. 22, 2024), https://www.ibm.com/topics/generative-ai.

making up content.[71] Moreover, the use of Gen AI in legal document drafting can raise ethical and legal considerations, particularly around liability and confidentiality, which must be carefully considered, and where appropriate, discussed with the client.[72] Most jurisdictions in Canada have directed that when artificial intelligence has been used in preparation of materials filed with the court, the materials must indicate how it was used.[73]

N. Legal Analytics

AI can be used to predict legal case outcomes, a practice known as predictive legal analytics. Through machine learning algorithms and NLP, AI can analyze historical case data and

---

71. Mata v. Avianca, Inc., 22-cv-1461 (PKC) (S.D.N.Y. Jun. 22, 2023).

72. Madison Shaner, *Potential Issues and Liabilities of Using Generative AI for Legal Document Drafting*, MILGROM, DASKAM & ELLIS, (Sep. 11, 2023), https://www.milgromlaw.com/artificial-intelligence/potential-issues-and-liabilities-of-using-generative-ai-for-legal-document-drafting/.

73. *See*, e.g., Court of King's Bench of Manitoba, Practice Direction re: Use of Artificial Intelligence in Court Submissions (Jun. 23, 2023); Supreme Court of Yukon, Practice Direction General-29 re: Use of Artificial Intelligence Tools (Jun. 26, 2023); Alberta Courts, Notice to the Public and Legal Profession re: Ensuring the Integrity of Court Submissions When Using Large Language Models (Oct. 6, 2023); Supreme Court of Nova Scotia, Ensuring the Integrity of Court Submissions When Using Generative Artificial Intelligence ("AI") (Oct. 18, 2023); Superior Court of Qu. . .bec, Notice to Profession and Public re: Integrity of Court Submissions When Using Large Language Models (Oct. 24, 2023); Provincial Court of Nova Scotia, Use of Artificial Intelligence (AI) and Protecting the Integrity of Court Submissions in Provincial Court (Oct. 27, 2023); Federal Court (note - may have been updated more recently); Interim Principles and Guidelines on the Court's Use of Artificial Intelligence (Dec. 20, 2023); Notice to the Parties and the Profession re: The Use of Artificial Intelligence in Court Proceedings (Dec. 20, 2023); and Ontario Rules of Civil Procedure, R.R.O. 1990, Reg. 194, rules 61.11(1)(e)(v), 61.11(5), 61.12(3)(f)(v) and 61.12(5.3) (as amended as of Jan. 1, 2024)

discern insightful patterns that can be used to predict the potential outcomes of future cases.[74]

Legal analytics can predict the outcome of motions based on inputs such as counsel, judges, jurisdiction, case type, facts, claims, and other metrics. Parties can use predictive analysis to prepare for trial (or other stages of litigation) with a better understanding of their case's strengths, weaknesses, and overall probability of success. Such data can inform case strategy and considerations including whether to pursue settlement, or what a favourable settlement might look like.[75] AI also enables parties to most effectively deploy their limited resources and avoid wasting resources on strategies that are unlikely to advance case objectives.

Legal analytics collect data from previous cases. Using machine-learning algorithms, the AI system analyzes this data to identify patterns and correlations. For example, it might find that certain arguments are more likely to be successful in certain types of cases, or that certain judges are more likely to prefer the precedents of certain other judges or rule in a particular way on certain kinds of cases. Based on these patterns and correlations, the AI system can predict the likely outcome of a new case. For instance, given the facts of a new case and the arguments being made, the AI system can estimate the probability of winning the case. As more case data becomes available, the AI system continuously updates its model, making its predictions more accurate over time.

---

74. *Top 5 Predictive Analytics Models and Algorithms*, INSIGHTSOFTWARE, (Jan. 1, 2023), https://insightsoftware.com/blog/top-5-predictive-analytics-models-and-algorithms/.

75. Prabhjot Singh, *Predictive Analytics for Case Outcomes – A Brief*, LINKEDIN, (Aug. 16, 2023), https://www.linkedin.com/pulse/predictive-analytics-case-outcomes-brief-prabhjot-singh.

Judicial analytics focus on the behaviour and decisional trends of individual judges. Armed with a better understanding of how a court is likely to rule, parties can tailor arguments with a more favourable history in a certain jurisdiction or before a certain judge, thereby avoiding arguments or positions on which a particular judge has not tended to rule favourably. For example, if a judge consistently denies motions to compel disclosure of TAR methodology absent a demonstrated material deficiency in the producing party's production, a requesting party will likely devote more time to negotiating and conferring with opposing counsel to reach a resolution, rather than engaging in costly motion practice in which they are unlikely to prevail.

Lawyer analytics sample metrics related to individual lawyers, such as success rates and experience with different types of cases. For example, if opposing counsel has never tried an obviousness case, that weakness may inform arguments and strategy in pharmaceutical patent litigation. If opposing counsel consistently avoids trials or consistently loses cases that go to trial, they may be more open to settlement discussions. Similarly, law firm analytics can highlight a firm's experience (or lack of experience) with certain practice areas and may help prospective clients choose the best or most experienced representation for their case.

While AI can identify trends, it cannot necessarily explain them. Nor can it account for every possible input, such as a litigator's performance or a judge's mood on a particular day. To serve as an input, a variable must be capable of measurement and documentation, so AI cannot account for certain soft factors such as characteristics or experiences of jurors that are not reflected on questionnaires or exposed through voir dire. Certain inputs may also be confidential and thereby elude a model that learns on publicly available data. It is important to note that these predictions are based on statistical patterns and should

not replace human judgment and expertise. Lawyers still need to interpret the results and consider other factors that may impact the case outcome.

O. Employment and Human Resources

Employment and Human Resources (HR) cover a wide range of legal issues, which include discrimination, harassment, wrongful termination, employment contracts, workplace safety, employee benefits, leave issues, and privacy rights. As previously mentioned, AI can add significant efficiency to litigation-related tasks such as document analysis and review. However, AI systems can also assist HR departments in other ways.

AI can be used to monitor and ensure compliance with various employment laws. For example, it can help track employee working hours to ensure compliance with labor laws or monitor communications for potential harassment or discrimination issues.[76]

AI tools can help automate parts of the recruitment and hiring process, such as screening résumés or scheduling interviews. However, when used for such purposes, it is essential to ensure that these tools are being used in ways that comply with applicable anti-discrimination laws.

AI-powered platforms can facilitate negotiations between parties, helping them find mutually agreeable solutions without the need for court intervention. These platforms use algorithms to propose solutions based on the parties' preferences and priorities.

---

76. *The Role of AI in Creating a More Inclusive and Supportive Work Environment*, SODALES SOLUTIONS, (Aug. 27, 2024), https://www.sodalessolutions.com/the-role-of-ai-in-creating-a-more-inclusive-and-supportive-work-environment/.

Finally, AI can analyze employee data to predict potential issues, such as employee turnover or performance issues. This can allow HR and management to proactively address these issues before they become bigger problems.

P. Legal Spend and Legal Operations Analytics

The quality and effectiveness of legal services can be greatly improved by incorporating business principles and technology into legal operations[77] to maximize value. This transformation centres on legal analytics,[78] which involves collecting and analyzing data to improve decision-making accuracy and performance evaluation. Strategic control over legal expenditures[79] is important to achieve this goal, with careful oversight and comprehensive reporting of all financial outlays related to legal proceedings.

As previously discussed, AI can assist in matter management by automating document review, contract analysis, and legal research tasks. Legal Operations Analytics can provide important insights into past litigation data, enabling legal teams to assess the likelihood of success, anticipated costs, and potential settlement options.

AI can streamline file and cost management by automating client invoice review and approval processes. It can identify billing discrepancies, ensure adherence to billing guidelines, and

---

77. ACC Legal Operations, *About Corporate Legal Operations*, ASSOCIATION OF CORPORATE COUNSEL, (July 21, 2020), https://www.acc.com/resource-library/acc-legal-operations.

78. Simple Legal, *What is Legal Analytics and How Can Legal Ops Use Them*? LEXOLOGY, (NOV. 30, 2022), https://www.lexology.com/library/detail.aspx?g=0447f6f0-0de1-4fdf-afb5-cb667e87e9eb (last visited Feb. 19, 2025).

79. *What is Legal Spend Management?* THOMSON REUTERS, (Jul. 2, 2024), https://legal.thomsonreuters.com/en/insights/articles/what-is-legal-spend-management.

help in budget forecasting for legal projects. This leads to better cost control, reduced billing errors, and more accurate financial projections.

With client consent[80], law firms can use AI-powered analytics to study client data, which can help to recognize patterns in their behaviour, preferences, and requirements. Matching services with client expectations improves client satisfaction and retention. Additionally, AI can provide insights into market trends and competitive intelligence, enabling law firms to make better-informed business decisions.

AI-powered chatbots can quickly answer compliance and ethics questions with human oversight, offering reliable information and reducing the risk of non-compliant or unethical behaviour. These chatbots can also automate repetitive tasks such as regulatory updates and conflict checks, which allow legal professionals to concentrate on more complex or important duties.

Q. Predictive Policing and Risk Assessment in the Criminal Justice System

AI is increasingly being used in the criminal justice system for risk and recidivism assessment, particularly in predicting the likelihood of reoffending or determining the level of threat posed by a particular individual. Some jurisdictions use such AI to assess the risk posed by a defendant, including the likelihood of reoffending or failing to appear in court. These AI systems are generally designed to exclude factors such as race, gender, and

80. *See, e.g.*, *Ethics of Artificial Intelligence for the Legal Practitioner*, THE CANADIAN BAR ASSOCIATION, https://cba.org/resources/practice-tools/ethics-of-artificial-intelligence-for-the-legal-practitioner/?_gl=1*1m35f3y*_ga*NTM1MDE5MTQwLjE3NDI1Nzk5Nzc.*_ga_YTMHKDEBK2*MTc0MzYxMTc3Ni4yLjAuMTc0MzYxMTc3Ni42MC4wLjA.&_ga=2.97084823.904603345.1743611776-535019140.1742579977 (last visited Apr. 2, 2025)

socioeconomic status, thereby reducing potential bias in risk assessments, but these efforts have not been universally successful.[81]

Predictive policing algorithms use historical crime data to predict where, when, and what type of crimes are likely to occur.

However, the use of AI in these ways is not without controversy. Critics argue that these systems can reinforce existing biases in the criminal justice system, as they are often trained on data that may reflect historical and systemic bias. There is also concern about transparency, as the algorithms used are often proprietary and therefore not open to public scrutiny.[82]

R. Facial Recognition and Other Biometrics

Facial recognition and biometrics are increasingly being used in criminal cases due to their potential to provide purportedly objective and reliable evidence. However, their use also raises important legal and ethical considerations. [83]

Facial Recognition is a type of biometric technology that can identify or verify a person's identity by comparing and analyzing patterns based on the person's facial features with pictures contained in large photo databases. Facial recognition can be

---

81. *See, e.g.*, Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

82. Hans de Bruijn et al., *The Perils and Pitfalls of Explainable AI: Strategies for Explaining Algorithmic Decision-Making*, 39 GOVERNMENT INFORMATION QUARTERLY, (2022), https://www.sciencedirect.com/science/article/pii/S0740624X21001027.

83. Jon Bongiorno, *Facial recognition technology gains popularity with police, intensifying calls for regulation*, THE CANADIAN PRESS, https://www.cbc.ca/news/politics/facial-recognition-ai-police-canada-1.7251065 (last visited Apr 2, 2025).

used for various purposes, such as identifying suspects in criminal investigations, verifying identities in immigration cases, or finding missing persons. However, facial recognition technology has been criticized for its potential for misuse, its bias, and its potential to infringe on privacy rights. There are concerns about accuracy in relation to identifying individuals from certain racial and ethnic groups that are less well represented in the data used to train these systems. There have been several instances in the US where persons of color were misidentified and arrested for crimes they did not commit.[84]

Biometrics is the measurement and statistical analysis of people's unique physical or behavioural characteristics. This can include fingerprints, voice patterns, iris scans, and more. In legal cases, biometric data can provide powerful evidence due to its unique and individual nature. For example, fingerprint or DNA evidence can play a crucial role in criminal cases. However, as with facial recognition, the use of biometrics raises concerns about privacy, consent, and data security.[85]

The use and accumulation of facial recognition and biometrics data by law enforcement agencies in Canada has been a subject of some debate. Some police forces have used facial recognition technology in criminal investigations.[86] The RCMP

84. Christina Carrega, *Facial Recognition Technology and False Arrests: Should Black People Worry?* CAPITAL B, (Sep. 14, 2023), https://capitalbnews.org/facial-recognition-wrongful-arrests/. *See* also Jon Brodkin, *Black man wrongfully jailed for a week after face recognition error, report says*, ARS TECHNICA, https://arstechnica.com/tech-policy/2023/01/facial-recognition-error-led-to-wrongful-arrest-of-black-man-report-says/ (last visited Apr. 2, 2025).

85. *Biometrics*, INNOVATRICS, https://www.innovatrics.com/glossary/biometrics/#:~:text=Biometrics%20is%20the%20measurement%20and,is%20evolving%20all%20the%20time (last visited Feb. 19, 2025).

86. Joe Bongiorno, *Facial Recognition Technology Gains Popularity With Police, Intensifying Calls for Regulation*, THE CANADIAN PRESS, (Jun. 30, 2024),

maintains a national database of fingerprints and criminal records, known as the Canadian Police Information Centre. The Canadian Border Services Agency uses biometric data, such as fingerprints and facial scans, as part of its identity verification process for travelers. Concerns have been raised about the potential for racial bias in facial recognition algorithms, as well as the potential for the accumulation of this data to infringe on individuals' privacy rights.

In Canada, the use of facial recognition and biometrics in legal cases is regulated by various federal and provincial laws. The *Privacy Act* at the federal level and various provincial privacy laws govern the collection, use, and disclosure of personal information by government organizations. These laws require that individuals be informed of and consent to the collection of their personal information, which includes biometric data. Given the complex ethical and legal issues associated with these technologies, their use in legal cases in Canada is an evolving area of law and policy.

IV. BENEFITS OF ARTIFICIAL INTELLIGENCE

The use of AI has many obvious potential benefits for the legal industry, most notably greater efficiency, reduced costs, and improved quality and consistency in appropriate circumstances.

A. Better Quality and Greater Consistency

Data quality and consistency are critical in the legal domain, where data-driven insights and decisions can significantly influence case outcomes, client relations, and compliance with rules and regulations. Consider the use of AI for legal research. Lawyers access and search vast databases to research statutes, case

---

https://www.cbc.ca/news/politics/facial-recognition-ai-police-canada-1.7251065.

law, and regulatory texts, to gather information essential for building cases, advising clients, and making informed legal decisions. If the data being searched is riddled with inaccuracies or inconsistencies, or is missing cases, the results can lead to misguided legal strategies, misinterpretation of laws, and, ultimately, unfavourable outcomes in proceedings. For an AI system to be effectively used for research, maintaining data integrity is critical to ensuring quality and consistency in the results.[87] This is often easier to attain using computer-assisted processes rather than purely manual ones. One clear example of where technology-assisted processes have been shown to surpass manual processes is in the review of documents for production in litigation.[88]

B. Increased Defensibility

When an AI system is defensible, it means its decisions are transparent, interpretable, and justifiable. This can build trust among lawyers, clients, and the judicial system, thereby enhancing the credibility of both the AI tool and the legal practitioners using it. While not all AI systems are transparent, many AI methods can be readily subjected to objective validation processes to demonstrate their validity and the reliability of their outputs. Again, this has been particularly true with the use of

87. *Building Trust in AI: Why Data Integrity is Essential in SAP ERP Systems*, INNOVAPTE, https://innovapte.com/blog/building-trust-in-ai-the-role-of-data-integrity/ (last visited May 30, 2025).

88. Maura R. Grossman & Gordon V. Cormack, *Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review*, 17 RICH. J.L. & TECH. 11 (2011), https://scholarship.richmond.edu/jolt/vol17/iss3/5/ (last visited September 23, 2024).

TAR in eDiscovery, where the calculation of metrics such as recall and precision are common.[89]

C. *Greater Efficiency*

The use of AI systems facilitates the effective use of resources by automating tasks and providing accurate insights, allowing legal professionals to focus on more complex, value-added aspects of their work. Through the automation of repetitive manual and often time-intensive processes and tasks, AI systems offer practitioners an invaluable commodity: saved time. This efficiency can contribute meaningfully to the overall productivity and profitability of legal practice.

D. *Permitting Lawyers to Focus on Higher-Level Work*

AI systems that have demonstrated validity and reliability can streamline various repetitive, time-consuming tasks that lawyers have traditionally performed, such as document review, due diligence, contract analysis, proofreading, and legal research. As a result, efficiencies are gained that allow lawyers to redirect their efforts from these time-consuming tasks to high-level, intellectual work requiring judgment that adds more value to clients and the legal practice by elevating the level of service provided and ultimately saving on costs.

---

89. *See, e.g.*, 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 (2014), https://www.fclr.org/fclr/articles/pdf/comments-implications-rule26g-tar-62314.pdf (last visited Feb. 19, 2025); Gordon V. Cormack, *Evaluation of Machine-Learning Protocols for Technology-Assisted Review in Electronic Discovery*, SIGIR '14: Proc. of the 37th Int'l ACM SIGIR Conf. on Res. & Dev. In IR, 153 (2014), https://dl.acm.org/doi/10.1145/2600428.2609601 (last visited Feb. 19, 2025). *But see* Maura R. Grossman & Gordon V. Cormack, *The eDiscovery Medicine Show*, 18 OHIO ST. TECH. L.J. 1 (2021), https://moritzlaw.osu.edu/sites/default/files/2022-01/THE%20EDISCOVERY%20MEDICINE%20SHOW.pdf (last visited Feb. 19, 2025).

E. Cost Savings

Through automation, legal professionals can reduce the cost of previously manual tasks and focus on more complex, high-value work, thereby increasing overall productivity and reducing the hours billed for time-consuming and primarily administerial tasks.[90] For example, document reviews that previously required large teams of contract reviewers and many months to complete can now be done in just a couple of weeks, by a smaller team, by leveraging AI-based TAR tools.[91] In this scenario, the cost savings can be passed on to the client, and the lawyer's time is freed up to focus on quality control and other work important to the case. Furthermore, AI systems can be used toreduce human error, particularly in tasks that involve large datasets or repetitive processes, such as document review.[92] By minimizing human error, AI helps avoid potential costs associated with fixing mistakes and mitigating any legal issues that arise from such mistakes.[93]

F. Potential Increases in Access to Justice

Embracing AI within the legal domain holds substantial promise for amplifying access to justice for a wider group of

---

90. *Law Firm Automation: The Value It Brings To Your Firm*, LPS, https://legalpracticesupport.co.uk/integrations/law-firm-automation-the-value-it-brings-to-your-firm/ (last visited Feb. 19, 2025).

91. Duke Law, *Technology Assisted Review (TAR) Guidelines*, BOLCH JUDICIAL INSTITUTE, (Jan. 2019), https://edrm.net/wp-content/uploads/2019/02/TAR-Guidelines-Final.pdf.

92. Sasha Berson, *AI for Lawyers Guide: Is AI the Future of the Legal Industry?* GROW LAW FIRM, (Mar. 27, 2024), https://growlawfirm.com/blog/ai-for-lawyers-guide.

93. *How to Use AI to Avoid Human Error and Save Costs in Your Manufacturing Operations*, TUPL, (Nov. 2, 2023), https://www.tupl.com/blog/how-to-use-ai-to-avoid-human-error-and-save-costs-in-your-manufacturing-operations/.

individuals.[94] Streamlining various aspects of civil litigation including, for example, the drafting of court filings, opens the door to the justice system for a larger and more diverse population. Furthermore, legal practitioners, once weighed down by heavy caseloads, gain the capacity to manage additional cases, thereby extending essential legal assistance to more clients. Similarly, smaller law firms that once struggled to compete with larger ones may now have access to the same advanced legal research tools and analytics, leveling the playing field and enhancing the quality of legal representation.[95]

V. CONSIDERATIONS WHEN USING ARTIFICIAL INTELLIGENCE

While AI presents tremendous opportunities for productivity and innovation, its practical application requires a solid understanding of its limitations and challenges. As AI tools bcome intertwined with the fabric of legal practice, understanding their intricacies is both beneficial and essential. Some of the challenges and considerations that apply to legal applications are discussed in this section.

A. Data Quality: Not All Data is Created Equal

To mitigate issues such as bias or invalid predictions, it is necessary to use comprehensive and representative datasets for training AI systems.[96] Data scrubbing and imputation

94. Joel Tito, *How AI Can Improve Access to Justice*, CENTRE FOR PUBLIC IMPACT, (Oct. 23, 2017), https://www.centreforpublicimpact.org/insights/joel-tito-ai-justice.

95. Ray Biederman, *Smaller Law Firms, Big Technology: Why e-Discovery Isn't Just for the Legal Giants*, RELATIVITY BLOG, (Jul. 24, 2024), https://www.relativity.com/blog/smaller-law-firms-big-technology-why-e-discovery-isnt-just-for-the-legal-giants/.

96. Emilio Ferrara, *The Butterfly Effect in Artificial Intelligence Systems: Implications for AI Bias and Fairness*, 15 MACHINE LEARNING WITH APPLICATIONS,

techniques can also be used to cleanse data and estimate missing values in the dataset. However, these techniques have their own limitations and must be applied carefully. Ultimately, the quality and completeness of the data used to train AI systems are critical determinants of their performance and fairness.

At its core, AI is based on data. Therefore, data quality and completeness are crucial for accurate and reliable results.[97] Incomplete data can lead to inaccuracy, bias, and/or overfitting.[98] Incomplete data can also lead to legal and ethical issues, particularly if an AI system's decisions or predictions systematically and negatively impact certain individuals or groups due to gaps or errors in the data.

B. Correlation vs. Causation: Seeing Patterns vs. Understanding Them

When diving into data analysis, particularly with AI, it is helpful to understand the difference between two foundational concepts: correlation and causation.

Correlation refers to an observed relationship or connection between two or more variables. When one variable changes, there is a consistent, observable pattern in the other, either in the same or opposite direction. For example, a rise in online searches for winter coats might correlate with colder months.

(2024), https://www.sciencedirect.com/science/article/pii/S266682702400001X (last visited Feb. 19, 2025).

97. Gary Drenik, *Data Quality For Good AI Outcomes*, FORBES, (Aug. 15, 2023), https://www.forbes.com/sites/garydrenik/2023/08/15/data-quality-for-good-ai-outcomes/.

98. Overfitting occurs where an AI model learns to perform well on its training data but performs poorly on new, unseen data. This is because the model has effectively memorized the training data, including its gaps and inconsistencies, rather than learning to properly generalize from it. *What is Overfitting?* AWS, https://aws.amazon.com/what-is/overfitting/ (last visited Feb. 19, 2025).

However, the correlation does not necessarily mean that colder months caused the increase in searches.

Causation implies a cause-and-effect relationship between variables. Using the previous example, if causation is shown, then we can assume that online searches for winter coats will increase because of the presence of colder months. In the context of AI, identifying causal relationships can be challenging, as AI models are typically trained to find correlations between variables.

Understanding the difference between correlation and causation is helpful in interpreting AI outputs. Misinterpreting correlation as causation can lead to flawed decision-making and inaccurate predictions. Hence, human oversight and domain knowledge are crucial in interpreting the results generated by AI systems.

C. Bias: Unwanted Baggage in Artificial Intelligence

Bias in AI refers to systematic errors or prejudices in the outputs produced by AI systems. It can be categorized into two types: intentional and unintentional bias.

Intentional bias occurs when an AI system is deliberately designed to favor certain outcomes over others. For example, a loan-approval algorithm might be intentionally biased to favor certain types of applicants (e.g., those with higher credit scores) if it has been specifically programmed to do so. While intentional bias can sometimes be used for legitimate purposes, such as promoting fairness or diversity, if misused, it can also lead to discriminatory outcomes.

Unintentional bias occurs when an AI system produces biased or unfair results due to issues in the training data or errors in the design of the algorithm. For example, suppose a facial recognition system is trained predominantly on images of light-

skinned individuals. In that case, it may perform poorly on individuals with darker skin tones.

Bias in AI can significantly affect the outcomes and predictions of a system. It is therefore necessary to take steps to identify and mitigate bias in AI, such as using representative and diverse training data, regularly auditing and testing AI systems for bias, and incorporating fairness metrics into the design of AI algorithms. Recognizing and addressing these biases is important, especially in a legal context where equity and impartiality are core principles.[99]

D. Equitable Access and Other Fairness Considerations

AI systems have the potential to help close the access-to-justice gap. At the same time, there is a fear that AI will increase inequities, favoring those who can afford the benefits it provides. This could further exacerbate existing disparities, leaving marginalized communities behind.[100] A concerted effort is needed to ensure that a two-tiered system is avoided and that providers strive to close the gap in Canada's access-to-justice problem.

Fairness in AI systems refers to the absence of discrimination or favoritism toward any individual or group based on protected characteristics such as race, gender, age or religion.[101] For

99. *AI Bias: Definition, Occurrence, Types, Causes, and Prevention*, HOLISTIC SEO, (Jul. 28, 2023), https://www.holisticseo.digital/ai/ethics/bias/.

100. *See* ABDI AIDID & BENJAMIN ALARIE, THE LEGAL SINGULARITY: HOW ARTIFICIAL INTELLIGENCE CAN MAKE LAW RADICALLY BETTER (Univ. of Toronto Press 2023) at 146–150; Drew Simshaw, *Access to A.I. Justice: Avoiding an Inequitable Two-Tiered System of Legal Services*, 24 YALE JOURNAL OF LAW & TECHNOLOGY 150 (2022).

101. Emilio Ferrara, *Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies*, MULTIDISCIPLINARY DIGITAL

instance, an AI tool used to predict the likelihood of recidivism should not disproportionately categorize persons of color as high-risk due to biases in the training data or other aspects of the algorithm.[102]

Equitable access to AI in the justice system means that datasets close societal gaps and minimize inequity by making sure that AI models are trained on appropriate and representative data that provide relevant, accurate, and unbiased outputs.[103]

E. Defensibility and Validation: Ensuring the Credibility, Consistency, and Safety of Artificial Intelligence

Decisions based on AI systems must be defensible to comply with legal principles, industry standards, and ethical guidelines. Defensibility concerns the ability to explain, justify, and defend the decisions made by the AI system. This involves ensuring that, whenever possible, the AI system is built and trained in a transparent, interpretable, and comprehensible way. This is particularly important in the legal context where the decisions and actions taken based on AI recommendations can have significant implications.

When transparency is not possible, independent validation becomes even more important. Validation refers to an objective assessment of whether the AI is working as intended (i.e., valid) and produces accurate results under substantially similar

---

PUBLISHING INSTITUTE, 6 SCI 3, (2024), https://www.mdpi.com/2413-4155/6/1/3 last visited Feb. 19, 2025).

102. Gideon Christian, *Artificial Intelligence, Algorithmic Racism and the Canadian Criminal Justice System*, SLAW, (Oct. 26, 2020), https://www.slaw.ca/2020/10/26/artificial-intelligence-algorithmic-racism-and-the-canadian-criminal-justice-system/.

103. *See supra* note 93.

circumstances (i.e., consistency and reliability).[104] This typically involves testing the system on a separate validation dataset not used in the training process to evaluate the system's performance and generalizability to new, unseen data.[105] Validation should also consider other aspects such as fairness (i.e., the system should not show bias towards or against identified groups), robustness (i.e., the system should perform well even under non-ideal conditions or when it is subject to intentional efforts to cause it to malfunction), and safety (i.e., the system should not cause harm or unanticipated and undesired outcomes).[106]

F. Opaqueness

Opaqueness refers to the lack of transparency or clarity in an AI system's predictions or decisions. AI systems that are opaque are often referred to as "black box." AI systems, particularly those based on complex machine-learning algorithms such as deep learning, often involve complicated computations and vast amounts of data.[107] Testing is almost always needed to ensure the credibility and reliability of the system's outputs,

104. Lalli Myllyaho et al., *Systematic Literature Review of Validation Methods for AI Systems*, 181 JOURNAL OF SYSTEMS AND SOFTWARE, (2021), https://www.sciencedirect.com/science/article/pii/S0164121221001473 (last visited Feb. 19, 2025).

105. *What are the differences between training, validation, and testing sets in machine learning?* LINKEDIN, https://www.linkedin.com/advice/1/what-differences-between-training-validation-testing-umoje (last visited Feb. 19, 2025).

106. Christopher Srinivasa, *Overview of Model Validation Pipeline*, BOREALIS AI, (May 27, 2022), https://www.borealisai.com/research-blogs/overview-model-validation-pipeline/.

107. *What is AI (artificial intelligence)?* MCKINSEY & COMPANY, (Apr. 3, 2024), https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-ai.

particularly when they cannot be explained.[108] For example, if an AI system is used to recommend a patient's treatment in healthcare, doctors and patients would want to understand why that recommendation was made and the degree of confidence the AI system has in the accuracy of the prediction. Similarly, in the legal or financial sectors, explanations may be required for decisions that have significant legal implications in addition to proof of validity and reliability.

Efforts to address the opacity problem in AI often focus on developing techniques for explainable AI (XAI) or interpretable AI. These are AI systems that are not only capable of making decisions or predictions, but also of providing explanations for those decisions that are understandable to humans.[109] This is a growing field in computer science.

G. *Accountability: Ensuring Artificial Intelligence Operates Responsibly and Ethically*

As AI technology rapidly advances, significant ethical and accountability concerns arise that must be addressed. Current

---

108. Ramesh Srivatsava Arunachalam, *Auditing and Validating AI Systems for Reliability and Validity*, LINKEDIN, (Oct. 11, 2023), https://www.linkedin.com/pulse/auditing-validating-ai-systems-reliability-validity-ramesh-iox9c?trk=public_post_main-feed-card_reshare_feed-article-content#:~:text=The%20Twin%20Pillars%3A%20Reliability%20and,correctness%20of%20the%20system's%20output.

109. The Technology and Privacy Unit of the European Data Protection Supervisor (EDPS), *TechDispatch on Explainable Artificial Intelligence*, THE EUROPEAN DATA PROTECTION SUPERVISOR, (2023), https://www.edps.europa.eu/system/files/2023-11/23-11-16_techdispatch_xai_en.pdf (last visited Feb. 20, 2025).

AI systems lack a fundamental quality that humans possess: judgement.[110] This means that:

- AI systems should be designed and used in a way that treats all individuals and groups fairly. They should not discriminate against, or harm particular groups based on legally protected characteristics.[111]
- AI systems should operate transparently to the degree possible. Their decision-making processes should be explainable and understandable by humans, at least at some level of abstraction.[112]
- There must be clear accountability for the decisions made by AI systems. This involves establishing a specific person or entity that is responsible when an AI system makes a mistake or causes harm. It also involves creating mechanisms for appealing the decisions of an AI system and auditing and overseeing the use of AI.[113]

---

110. Peter Gärdenfors Ph.D., *Why AI Lacks Judgment*, PSYCHOLOGY TODAY, (Jun. 5, 2023), https://www.psychologytoday.com/ca/blog/what-is-a-human/202306/why-ai-lacks-judgment.

111. *What About Fairness, Bias and Discrimination?* INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-about-fairness-bias-and-discrimination/ (last visited Feb. 20, 2025).

112. Sajid Ali et al., *Explainable Artificial Intelligence (XAI): What We Know and What is Left to Attain Trustworthy Artificial Intelligence*, 99 INFORMATION FUSION, (2023), https://www.sciencedirect.com/science/article/pii/S1566253523001148 (last visited Feb. 20, 2025).

113. *AI Risk Management: Transparency & Accountability*, LUMENOVA AI, (May 28, 2024), https://www.lumenova.ai/blog/ai-risk-management-importance-of-transparency-and-accountability/.

- AI systems must comply with relevant laws and regulations regarding data protection. They must use data in ways that show respect for individuals' privacy rights.[114]
- AI systems should be designed and used in ways that ensure the safety and security of individuals and society.[115]

H. Privacy and Security

Protection of personal and confidential information and prevention of unauthorized access are at the forefront of AI's integration into legal practice. There is a significant concern that private or confidential information may be exposed in ways that can violate solicitor-client privilege or privacy regulations. As AI systems and models evolve, so will the number and sophistication of nefarious methods to hack into data and algorithms, affecting the trustworthiness of their results.[116] It is crucial to be aware of some of the threats currently at play, and to remain current with respect to known privacy risks.[117]

---

114. Office of the Privacy Commissioner of Canada, *A Regulatory Framework for AI: Recommendations for PIPEDA Reform* (2020), https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011.

115. Microsoft AI, *Putting Principles Into Practice: How We Approach Responsible AI at Microsoft*, MICROSOFT, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.microsoft.com/cms/api/am/binary/RE4pKH5 (last visited Feb. 20, 2025).

116. Brett Cohen, *The Dark Side of AI: How Hackers are Leveraging Technology to Their Advantage*, EMAGINEHEALTH, (May 3, 2023), https://www.emaginehealth.com/blog/nefarious-ai-hacking-websites/

117. Office of the Privacy Commissioner of Canada, *Expectations: OPC's Guide to the Privacy Impact Assessment Process*, https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/#wb-cont (last visited Feb. 20, 2025).

Many AI systems rely on large amounts of personal data to function effectively. It is essential to ensure that this data is collected with consent, used only for the purpose(s) for which it was collected, and used appropriately and equitably. Strong data governance practices and anonymization techniques can help protect individuals' PII.[118]

Like any other software systems, AI systems can be vulnerable to cyberattacks of all sorts. Implementing robust security measures to protect these systems from threats is important.[119] Further, since legitimate AI technology that is widely available can be used maliciously, such as by creating deepfakes or through adversarial attacks, such systems can be deceived through subtle modifications of input data. Accordingly, it is essential to consider security in AI design and to ensure that robust processes are in place to prevent such attacks.[120]

118. Barkha Bathija, *How Data Anonymization Can Strengthen Data Privacy*, SERVICENOW, (Jan. 27, 2023), https://www.servicenow.com/blogs/2023/data-anonymization-strong-data-privacy.

119. Tshedimoso Makhene, *What are robust security measures?* PAUBOX, (May 8, 2024), https://www.paubox.com/blog/what-are-robust-security-measures#:~:text=The%20potential%20consequences%20of%20not%20implementing%20robust%20security%20measures%20include,operations%2C%20and%20legal%20liabilities%20resulting.

120. *What are deepfakes?* MALWAREBYTES, https://www.malwarebytes.com/cybersecurity/basics/deepfakes (last visited Feb. 20, 2025).

I. Authentication and Admissibility Issues

The field of law requires both the validity and reliability of evidence and information.

Authentication refers to the process of verifying the reliability and integrity of data or information,[121] i.e., is it what it purports to be? In the context of AI, authentication might involve validating the AI algorithm, verifying the data used to train the AI and/or the system's output, and ensuring the AI system has not been tampered with.[122] Conversely, *admissibility* refers to whether the evidence is allowed to be presented in court. For AI-generated evidence to be admissible, it needs to be both relevant to the case at hand, shown to be accurate (i.e., valid and reliable), must not be unfairly prejudicial or misleading, and must comply with other legal standards.[123]

The validity and reliability of the AI system that generates evidence can be demonstrated by showing that the AI system has been independently verified (e.g., peer reviewed) and is widely accepted and used in its field, that it is based on sound scientific principles, and that it produces accurate and consistent results. An example of evidence that would not meet

---

121. JEREMY FAIRCLOTH, ENTERPRISE APPLICATIONS ADMINISTRATION: THE DEFINITIVE GUIDE TO IMPLEMENTATION AND OPERATIONS, Chapter 5 – Information Security 175–220 (2014), *available at* https://www.sciencedirect.com/topics/computer-science/authentication-information#:~:text=Authentication%20is%20the%20process%20of,on%20a%20number%20of%20factors (last visited Feb. 20, 2025).

122. *Authenticating AI-Generated Content: Exploring Risks, Techniques & Policy Recommendations,* INFORMATION TECHNOLOGY INDUSTRY COUNCIL, (Jan. 2024), https://www.itic.org/policy/ITI_AIContentAuthorizationPolicy_122123.pdf (last visited Feb. 20, 2025).

123. Paul W. Grimm et al., *Artificial Intelligence as Evidence*, 19 Northwestern J. Tech. & IP Art. 3, (Dec. 2021), https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1349&context=njtip (last visited Feb. 20, 2025).

these standards is deepfakes. Deepfakes are altered or synthetic media in which some aspect of a person in an existing image, audio, or video is either partially or wholly replaced or manufactured. These manipulations can affect legal cases or public perception. As deepfake technology improves and it becomes harder to determine what is real, juries may start questioning the authenticity of properly admitted evidence, which in turn may have a corrosive effect on the justice system.[124] Verification tools, such as reverse image searches, are necessary countermeasures against such deceptive tactics.

Given the complexity and novelty of AI technology, there can be significant challenges in authenticating the output of AI systems and in demonstrating the admissibility of AI-generated evidence, leading to the increased need for forensic experts. This evolving area of law will likely continue to develop as the legal field increasingly uses AI.[125]

J. Ethical Considerations: Artificial intelligence's integration into law must align with the profession's ethical standards

AI's use in law brings several ethical considerations to the forefront, including:

---

124. This is known as the "liar's dividend." *See, e.g.*, Kaylyn Jackson Schiff et al., *The Liar's Dividend: The Impact of Deepfakes and Fake News on Trust in Political Discourse*, SocArXiv x43ph, CENTER FOR OPEN SCIENCE, https://ideas.repec.org/p/osf/socarx/x43ph.html (last visited Feb. 20, 2025). *See also* Rebecca A. Delfino, *Deepfakes on Trial: A Call Trial: A Call To Expand The Trial Judge's Gatekeeping Role To Protect Legal Proceedings from Technological Fakery*, 74 HASTINGS L. J. 297 (Feb. 2023), https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=4012&context=hastings_law_journal (last visited Feb. 20, 2025).

125. Evelina Gentry, *The Challenges of Integrating AI-Generated Evidence Into the Legal System*, AKERMAN, (Jun. 12, 2024), https://www.akerman.com/en/perspectives/the-challenges-of-integrating-ai-generated-evidence-into-the-legal-system.html.

1. Competency: Legal practitioners must maintain a proficient understanding of the AI tools they employ, ensuring accurate and ethical use.[126]

2. Protecting Confidentiality and Privilege: Any AI tool or system used in the legal context must uphold the sacred trust of client confidentiality and privileged information.[127]

3. Supervision: Continual oversight of AI systems is required, ensuring they align with legal and ethical standards.[128]

4. Quality of Legal Services: While AI can help automate certain legal tasks, it is essential to ensure that this does not compromise the quality of legal services. AI should

126. Section 3.1-4-.4A of the LSO *Rules of Professional Conduct* states that, "to maintain the required level of competence, a lawyer should develop an understanding of, and ability to use, technology relevant to the nature and area of the lawyer's practice and responsibilities. A lawyer should understand the benefits and risks associated with relevant technology, recognizing the lawyer's duty to protect confidential information set out in section 3.3, https://lso.ca/about-lso/legislation-rules/rules-of-professional-conduct (last visited Feb. 20, 2025).

127. Daniel Bron, *The Impact of AI on Client-Attorney Confidentiality: Protecting Privilege in the Digital Age*, SOLIDITY LAW, (May 9, 2023), https://www.linkedin.com/pulse/impact-ai-client-attorney-confidentiality-protecting-privilege.

128. Cornerstone Editors, *The crucial role of humans in AI oversight*, CORNERSTONE, https://www.linkedin.com/pulse/impact-ai-client-attorney-confidentiality-protecting-privilege (last updated Feb. 19, 2025).

> not replace the availability of competent legal advice from a human lawyer.[129]

These ethical issues highlight the need for careful oversight and regulation of AI in the legal field, and ongoing research and dialogue about the responsible and ethical use of AI in law. [130]

VI. CURRENT AND FUTURE REGULATORY RESPONSES

AI is a transformative technology. The global increase in the use of AI calls for regulation. While there are no Canadian federal regulations dedicated solely to AI, there are existing laws that touch on aspects of AI, and new laws and policies are being adopted to deal directly with AI risk. The proposed Canadian Privacy Legislation and Bill C-27, aim to fill this void. The use of AI is covered in Quebec's Law 25.

A. Canadian Privacy Legislation and Bill C-27

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) is a federal law that regulates the collection, use, and disclosure of personal information, and requires protection of such information against unauthorized use or theft.[131]

---

129. DRI Center for Law and Public Policy Artificial Intelligence Working Group, *Artificial Intelligence in Legal Practice: Benefits, Considerations, and Best Practices* (2024), DEFENSE RESEARCH INSTITUTE, https://www.dri.org/docs/default-source/dri-white-papers-and-reports/ai-legal-practice.pdf (last visited Feb. 20, 2025).

130. The European Union was the first jurisdiction to implement a comprehensive AI Law, European Union Artificial Intelligence Act (Jun. 13, 2024), *available at* https://artificialintelligenceact.eu/ai-act-explorer/.

131. EU AI Act, Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), *available at* https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/FullText.html (last visited Feb. 20, 2025).

Bill C-27 would repeal Part I of PIPEDA and replace it with a new Consumer Privacy Protection Act, which would allow organizations to de-identify and anonymize personal information, along with requirements for transparency around the use of automated decisions systems (including systems using predictive analytics or machine learning).[132]

Some Canadian provincial privacy laws correlate with Canadian federal privacy laws. One example is Quebec Law 25, which includes requirements for reporting on the use of biometric data and the reporting of security incidents.[133]

B. Artificial Intelligence and Data Act ("AIDA")

As part of Bill C-27, Canada introduced the Artificial Intelligence and Data Act ("AIDA") to regulate AI in the Canadian private sector.[134]

The proposed legislation includes requirements for persons responsible for high-impact systems to adopt measures to assess and mitigate risk of biased output or other harm stemming from the system.

The definition of a high-impact system under AIDA will be established by regulations. AIDA companion documentation provided by the government of Canada indicates that high-impact systems would be those that impact, among other things,

---

132. Parliament of Canada, Bill C-27, at CPPA ss. 62(2)(c) and 2(1) and Consequential and Related Amendments at s.4, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading (last visited Feb. 20, 2025).

133. *An Act to modernize legislative provisions as regards the protection of personal information*, SQ 2021 (as posted on Sep. 23, 2021), c 25, CANLII, https://canlii.ca/t/555nn (last visited Feb. 20, 2025).

134. *See* 39-Part 3 *Artificial Intelligence and Data Act* of the Bill C-27, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading (last visited Feb. 20, 2025).

health and safety, and human rights.[135] It has yet to be determined whether the AI algorithms used in eDiscovery applications would be considered high-impact systems, though that seems unlikely.

AIDA requires managers of a high-impact system to make available plain language descriptions of such systems, including how the system is intended to be used; the type of information used in the system; any decisions, recommendations, or predictions that are intended to be made; and mitigation measures.

AIDA also provides for the establishment of an Artificial Intelligence and Data Commissioner, monetary penalties and other provisions to enforce its requirements.

C. AI Regulations in Other Jurisdictions

The European Union's General Data Protection Regulation 2016/679 ("GDPR") is currently the most comprehensive data protection law in the world. It came into effect on May 25, 2018. The GDPR repealed the Data Protection Directive 95/46/EC, which was adopted to deal with the rise of the internet.[136] The GDPR protects the fundamental rights and freedoms of natural persons, their right to protection of personal data in balance with other fundamental human rights in the EU and international business.[137] The GDPR does not directly govern AI;

---

135. Additional companion document may be found at https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document (last visited Feb. 20, 2025).

136. EU General Data Protection Regulation 2016/679 art. 1, 94, 4(2), 22, 2016 O.J. (L 119) 1-88. (*enforceable May 25, 2018*), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (last visited Feb. 20, 2025).

137. Article 8(1) of the European Convention on Human Rights, 213 UNTS 221, Cmnd 8969 (1953), https://www.echr.coe.int/documents/d/echr/Convention_ENG (last visited Feb. 20, 2025).

however, it does address risk processes used by AI, including profiling, erasure, destruction of data, and automated individual decision making (ADM).[138]

The EU Artificial Intelligence Act (AI Act) is the first comprehensive AI legislation that has been approved, went into effect on Aug. 1, 2024, and is expected to be in full force by 2026.[139] The AI Act interacts directly with GDPR data governance scheme, as well as with other law enforcement directives and human rights rules regarding the design, development, and use of certain high-risk AI systems and also certain uses of remote biometric identification systems. The AI Act also aims to minimize the risk of algorithmic discrimination. The legislation identifies four levels of AI risk: (1) unacceptable risk, (2) high risk, (3) low or limited risk, and (4) minimal or no risk, with an emphasis on high-risk systems.[140]

The Illinois Biometric Information Privacy Act (BIPA) is an example of a jurisdiction-specific and industry-specific regulation in the United States, of which there are several. It is one of the most feared and challenged privacy laws after the Illinois Supreme Court unanimously held in *Rosenbach* v. *Six Flags Entm't Corp.* that private entities cannot collect biometric data from consumers without their consent.[141] The Court ruled

---

138. EU General Data Protection Regulation 2016/679 art. 4 (2), 22, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (last visited Feb. 20, 2025).

139. Draft on EU AI EPRS_BRI (2021) 698792_EN.pdf (*European Parliament Legislative Briefing on A.I. Proposal 1-2*). *See European Union Artificial Intelligence Act* (2024), https://artificialintelligenceact.eu/ai-act-explorer/ (last visited Feb. 20, 2025).

140. *The Four Risks of the EU's Artificial Intelligence Act: Is Your Company Ready?* FTI CONSULTING, https://www.fticonsulting.com/insights/fti-journal/four-risks-eus-artificial-intelligence-act (last visited Feb. 20, 2025).

141. Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186, 5, 6, 9. (Jan. 25, 2019), *available at* https://www.illinoiscourts.gov/Resources/

against Six Flags, finding that the collection of thumbprints without permission, despite no actual harm to the claimant, violated § 15 of BIPA.[142] A plethora of BIPA lawsuits have subsequently been brought and thus far, courts seem to be protecting critical privacy interest over business interests. For example, Texas has recently enforced biometric law in two cases brought against Meta Platforms, Inc., f/k/a Facebook and Google.[143] Unlike, the Illinois BIPA, the Texas Capture or Use of Biometric Identifier Act (CUBI) does not have a private right of action. CUBI can only be enforced by the state.[144] The *Meta Platforms* case focused more on lack of consent to use biometric systems on customers, while the *Google* case focused more on deceptive advertising around the use of the biometric information collected, including that Google uses that data for profiling.[145]

---

f71510f1-fb2a-43d8-ba14-292c8009dfd9/123186.pdf. (P. 34–35, "BIPA injury is not just technical, but real and significant with no recourse for the injury").

142. Illinois Biometric Information Privacy Act (740 ILCS 14/1 et seq) (West 2016), https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 (last visited Feb. 20, 2025). *(§ 15 of BIPA-regulates the retention, collection, disclosure and destruction of biometric data*).

143. State of Texas vs. Meta Platforms, Inc., f/k/a Facebook Inc. No. 22-0121, 20-24 (D. Tex. Filed Feb. 14, 2022), https://texasattorneygeneral.gov/sites/default/files/images/child-support/State%20of%20Texas%20v.%20Meta%20Platforms%20Inc. .pdf (last visited Feb. 20, 2025); Complaint, at 8-16, 49 State of Texas vs Google LLC CAUSE No. CV58999 (D. Tex. File Oct. 20, 2022), https://texasattorneygeneral.gov/sites/default/files/images/child-support/State%20of%20Texas%20v.%20Meta%20Platforms%20Inc. .pdf (last visited Feb. 20, 2025).

144. (CUBI) Tex. Bus. & Com. Code § 503.001 under (d), (b), (c) (1) (DTPA) (3); §17.41 *et seq.* § 17.46 (a) and (b), §17.47 (b); (Penalties) Tex. Civ. Prac. Rem. Code. 15.002 (a) (1). *See Biometric Identifier Act*, https://www.texasattorneygeneral.gov/consumer-protection/file-consumer-complaint/consumer-privacy-rights/biometric-identifier-act (last visited Feb. 20, 2025).

145. Mike Scarcella, *Texas Flights Google Deposition Bid in Biometric Privacy Lawsuit*, REUTERS (Jun. 26, 2024), https://www.reuters.com/legal/

New York has implemented a new law to regulate bias in the use of AI in hiring decisions. It became effective on July 5, 2023, and is known as the Automatic Employment Decision Tool (AEDT) law.[146] The bill requires that a bias audit be conducted on any automated employment decision tool prior to use of the tool. The law also requires employees and job candidates be notified of the use of the tool during the hiring process and be provided with an opportunity to opt out. Violations are subject to civil penalties.[147] These acts are representative of the approach the U.S. has generally taken, which has tended to be more localized and sector-specific than the approach taken in the EU and anticipated to be taken in Canada.[148]

VII. LOOKING AHEAD

A. Authentication and Admissibility Issues

Evidence has always been fundamental to justice. With the emergence of AI systems, we are seeing new types of evidence emerge, such as sophisticated deepfakes that require special attention and scrutiny. These new types of data are likely to increase the need for experts who can delve into the intricacies of AI-generated evidence to determine if it is authentic and

transactional/texas-fights-google-deposition-bid-biometric-privacy-lawsuit-2024-06-26/.

146. New York City, N.Y., Automated Employment Decision Tool, Local Law No. 144 (2021), https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9&Options=ID%7CText%7C&Search.

147. New York City, N.Y., Local Law No. 144 Int. No.1894-A (West 2021.

148. *See* The Artificial Intelligence and Data Act (AIDA) – Companion document, The Government of Canada, https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document (last accessed Apr. 2, 2025); *see supra* note 138.

suitable for admission into evidence.[149] As AI continues to advance, so too do the challenges of verifying the origin and integrity of digital evidence.[150] Litigators, in particular, need to stay abreast of legal developments in this area.

B. All Manner of Deepfakes

The rapid advancement of deepfake technology poses a pressing concern.[151] AI-generated audiovisual clips can be alarmingly convincing and capable of simulating real individuals' speech and movements. In the context of litigation, if a deepfake video can be presented as genuine evidence, it will seriously undermine the integrity of proceedings and impact court decisions. Likewise, litigants may challenge genuine evidence on the grounds that it could be AI-generated.

Lawyers may soon find themselves leaning on cutting-edge tools and experts to affirm the authenticity of evidence. The dangerous potential of deepfakes was illustrated when comedian Jordan Peele partnered with BuzzFeed to produce a video that seemingly had former U.S. President Barack Obama making startling comments.[152] Yet, the voice behind the revelations was

---

149. Paul W. Grimm et al., *Artificial Intelligence as Evidence*, 19 NORTHWESTERN J. TECH. & IP ART. 3, (Dec. 2021), https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1349&context=njtip (last visited Feb. 20, 2025); Maura R. Grossman et al., *The GPT Judge: Justice in a Generative AI World*, 23 DUKE L. & TECH. REV. 1 (2023), https://scholarship.law.duke.edu/dltr/vol23/iss1/1/ (last visited Feb. 20, 2025).

150. *Id*. (to both).

151. Mika Westerlund, *The Emergence of Deepfake Technology: A Review*, 9 TECH. INNOV. MGMT. REV. 39, 52, (Nov. 2019), https://doi.org/10.22215/timreview/1282 (last visited Feb. 20, 2025).

152. James Vincent, *Watch Jordan Peele use AI to Make Barack Obama Deliver a PSA About Fake News*, THE VERGE, (Apr. 17, 2018), https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed.

Peele's, highlighting how seeing is not necessarily believing anymore. As Gen AI technology evolves, the legal world must remain vigilant, ensuring that evidence remains genuine in an era where digital impersonations are freely available to anyone with a computer and Internet connection and increasingly easy, cheap, and seamless to produce.

To help detect fake audio and video, companies such as Microsoft and Google are researching and developing ways to help detect deepfakes. One example is Microsoft, which has added a feature to its Bing Image Generator to help determine whether pictures or videos were made by AI.[153] This feature uses a special tag with information about the provenance of the content, commonly referred to as watermarking. Google is developing something similar that will show if visual media was created by AI.[154]

C. Generative AI ("Gen AI")

Ongoing research and development efforts with respect to Gen AI are currently operating at a breakneck speed. Gen AI relies on a combination of deep learning and NLP trained on vast datasets—including data scraped from the Internet and large proprietary databases—to generate new material in response to a human prompt.[155] Gen AI quickly expanded from text (i.e., LLMs) to images, audio, and video. Moving forward, we can expect this technology to become more ubiquitous and easier to use, and hopefully more accurate. The quality of converting text to images, audio, or video (and

153. Kyle Wiggers, *Microsoft Pledges to Watermark AI-Generated Images and Videos*, TECHCRUNCH, (May 23, 2023), https://techcrunch.com/2023/05/23/microsoft-pledges-to-watermark-ai-generated-images-and-videos/?guccounter=1.

154. *Id*.

155. Kim Martineau, *What is Generative AI?*, IBM, (Apr. 20, 2023), https://research.ibm.com/blog/what-is-generative-AI.

converting images, audio, or video to text) will continue to improve. Meta's AudioCraft is a recent example of this technology.[156] AudioCraft consists of two primary models available to users, MusicGen and AudioGen. The MusicGen model allows users to generate music from text, whereas the AudioGen generates sound effects from text.[157] As described earlier, the creation of high-quality computer-generated images, audio, and video will make it more difficult to tell the difference between human versus computer-generated content. As we have already seen, computer-generated content also raises copyright infringement issues.[158] To date, most content created by Gen AI in response to human prompts has not been considered subject to copyright protection.[159]

D. Access to Justice

AI systems and solutions have the potential to help close the access-to-justice gap through the rise of "efficiencies, democratiz[ing] access to legal information, and help[ing] consumers solve their own legal problems or connect them with licensed

---

156. Janakiram MSV, *Meta's AudioCraft Can Turn Your Words Into Music*, FORBES, (Aug. 3, 2023), https://www.forbes.com/sites/janakirammsv/2023/08/03/metas-audiocraft-can-turn-your-words-into-music/.

157. *Id*.

158. Atreya Mathur, *Art-Istic or Art-Ificial? Ownership and Copyright Concerns in AI-Generated Artwork*, CENTER FOR ART LAW, (Nov. 21, 2022), https://itsartlaw.org/2022/11/21/artistic-or-artificial-ai/; Congressional Research Service, *Generative Artificial Intelligence and Copyright Law*, (Sep. 29, 2023), https://crsreports.congress.gov/product/pdf/LSB/LSB10922#:~:text=AI%20programs%20might%20also%20infringe,created%20%E2%80%9Csubstantially%20similar%E2%80%9D%20outputs.

159. Michael Sumner, *Artificial Intelligence Copyright Infringement Explained*, SCOREDETECT, (Updated Nov. 19, 2024), https://www.scoredetect.com/blog/posts/artificial-intelligence-copyright-infringement-explained.

professionals who can."[160] We can expect to see more individuals representing themselves in court using AI software to draft legal documents. AI solutions are being developed to improve various aspects of the legal process from intake to case management and judicial engagements.

E. Robotics

While AI refers to software, robotics generally involves hardware that perceives and acts in the physical environment. Robotics and AI are widely used in many industries, such as manufacturing, automotive, packaging, and surgery. Historically, programming a robot to complete a simple human task (e.g., cleaning up a spill) required sets of complex instructions to account for all the obstacles it might encounter in the real world. Due to advances in AI, robots can now access a large amount of data to assist in their decision making instead of requiring hard-coded instructions.[161] For example, Google's RT-2 robot incorporates LLMs, improving the robots reasoning and improvisation skills.[162] By leveraging the large data available in these models, the RT-2 robot can analyze and navigate the surrounding environment.

---

160. Drew Simshaw, *Access to A.I. Justice: Avoiding an Inequitable Two-Tiered System of Legal Services*, 24 YALE JOURNAL OF LAW AND TECHNOLOGY 150, (2022), https://yjolt.org/access-ai-justice-avoiding-inequitable-two-tiered-system-legal-services.

161. Mohsen Soori, Behrooz Arezoo, and Roza Dastres, et al., *Artificial Intelligence, machine learning and deep learning in advanced robotics, a review*, 54, 70 (2023), 3 Cognitive Robotics, SCIENCEDIRECT, https://doi.org/10.1016/j.cogr.2023.04.001 (last visited Feb. 20, 2025).

162. Kevin Roose, *Aided by A.I. Language Models, Google's Robots Are Getting Smart*, THE NEW YORK TIMES, (July, 28, 2023), https://www.nytimes.com/2023/07/28/technology/google-robots-ai.html, (last visited September 23, 2024).

F. General or Strong AI

IBM defines Strong AI or Artificial General Intelligence ("AGI") or General AI as "a theoretical form of AI used to describe a certain mindset of AI development. If researchers can develop Strong AI, the machine would require an intelligence equal to humans; it would have a self-aware consciousness that could solve problems, learn, and plan for the future."[163] According to most definitions, AGI would meet or exceed the capacity of humans at most if not all tasks. There is considerable debate in the field of computer science as to whether and when AGI will be achieved, with estimates ranging from several years to never.

Today, we engage primarily with narrow or weak AI systems designed for specialized tasks, such as analyzing legal documents or forecasting case outcomes. Looking ahead, we can see a time when AI becomes more advanced, where it would be equipped with cognitive expertise to tackle intellectual tasks that currently only a human can undertake. For the legal field, this paints a picture of a future where lawyers work alongside AI counterparts that can grasp the nuances and subtleties of laws and facts, and gleaning insights in seconds from massive volumes of data their AI colleagues processed instantaneously.

G. Superintelligence

As defined by Merriam Webster, superintelligence refers to "an entity that surpasses humans in overall intelligence or in some particular measure of intelligence."[164] This kind of AI is

---

163. *What Is Strong AI* (October 13, 2021), IBM, https://www.ibm.com/topics/strong-ai#:~:text=If%20researchers%20are%20able%20to,indistinguishable%20from%20the%20human%20mind (last visited September 23, 2024).

164. *Superintelligence Definition & Meaning*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/superintelligence (last visited Feb. 20, 2025).

often depicted in science fiction as AI systems that greatly exceed human capabilities and often lead to dystopian outcomes. Such leaps in AI capabilities would be revolutionary for every sector, including the legal world. Imagine a legal system empowered by an AI that could sift through every known legal document in moments, predict the outcome of court cases with astounding precision, and draft just and effective legislation. The rise of superintelligence raises pressing ethical questions such as how far we let our trust in machinery extend, and whether human lawyers and judges can be completely replaced by AI, or if there are values that dictate that certain decisions (e.g., child custody or criminal sentencing) remain human functions. But this is all speculation.

VIII. CONCLUSION

Artificial intelligence is already inextricably intertwined in—and will continue to be part of—the practice of law. This basic AI primer has identified most of the current legal applications and has presented a brief overview of their risks and benefits**.** There is little doubt that legal applications will continue to proliferate, and that ethical considerations will need to be considered when employing AI technologies in the practice of law.[165]

The AI world is currently on fast-forward, expanding AI use in virtually every industry. AI's benefits have already been amply demonstrated in the legal industry through greater efficiency, improved quality and consistency, and lower costs for clients. Conversely, AI's limitations and challenges also need to be considered to ensure legal AI applications operate responsibly and consistently with various codes of conduct for

165. *AI and Law: What are the Ethical Considerations?* CLIO, https://www.clio.com/resources/ai-for-lawyers/ethics-ai-law/ (last visited Feb. 20, 2025).

attorneys.[166] As we move forward, we can expect to see more legislation and policies being adopted globally to ensure the safety and soundness of AI's use.

166. Matic Pogladic, *AI in Law: Opportunities, Challenges, and Ethical Considerations for Lawyers*, AUTOGPT BY MINDSTREAM, (Mar. 13, 2024), https://autogpt.net/ai-in-law-opportunities-challenges-and-ethical-considerations-for-lawyers/.

COMMENTARY ON SHARING TRADE SECRETS WITH OTHER ORGANIZATIONS

A Project of The Sedona Conference Working Group on Trade Secrets (WG12)

Author

The Sedona Conference

Editors-in-Chief

David Almeling Vicki Cundiff

Managing Editor

Casey Mangan

Senior Editors

Dean Pelletier Dina Hayes

Contributing Editors

John Barry Kerri Braun Jonathan Engler
Cameron Fine Jim Flynn Daniel Forester
Amber Harezlak Astor Heaven Rob Isackson
Daniel Saeedi Heather Schroder

WG12 Judicial Advisor: Hon. Donald Parsons (Ret.)

Staff Editor: Craig Morgan

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 12. 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 Sharing Trade Secrets with Other Organizations*, 26 SEDONA CONF. J. 175 (2025).

PREFACE

Welcome to the August 2025 Final Version of The Sedona Conference's *Commentary on Sharing Trade Secrets with Other Organizations*, a project of The Sedona Conference Working Group 12 on Trade Secrets (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, artificial intelligence, 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 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 Brainstorming Group to develop this *Commentary* was launched in December 2021. Early drafts of this publication (including the Brainstorming Group's project charter) were a focus of dialogue at the WG12 Annual Meeting in Reston, Virginia, in September 2022, the WG12 Annual Meeting in Minneapolis, Minnesota, in September 2023, and the WG12 Annual Meeting in Phoenix, Arizona, in September 2024. 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, the Chair of the WG12 Steering Committee, and Victoria Cundiff, now Chair Emeritus of the

Steering Committee, who served as the Editors-in-Chief of this *Commentary*, and Dina Hayes and Dean Pelletier who served as the Senior Editors. I also thank everyone else involved for their time and attention during this extensive drafting and editing process, including our Contributing Editors John Barry, Kerri Braun, Jonathan Engler, Cameron Fine, Jim Flynn, Daniel Forester, Amber Harezlak, Astor Heaven, Rob Isackson, Daniel Saeedi, and Heather Schroder, and our Judicial Advisor, the Hon. Donald Parsons (Ret.). The drafting process for this *Commentary* has also been supported by the entire WG12 Steering Committee.

The statements in this *Commentary* are solely those of the non-judicial 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 artificial intelligence and the law, electronic document management and discovery, cross-border discovery and data protection law, international data transfers, data security and privacy liability, 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. Information on membership and a description of current Working Group activities is available at https://www.thesedonaconference.org/wgs.

Kenneth J. Withers
Executive Director
The Sedona Conference
August 2025

TABLE OF CONTENTS

I. INTRODUCTION

Capitalizing on economic benefits of a trade secret often requires the owner to disclose the trade secret to an outsider for evaluation, use or regulatory approval. A key aspect of such disclosure, or sharing, is that the trade secret be reasonably protected under the corresponding circumstances.

Despite the recognized need to share information in the real world, little written guidance has been provided to entities that need or want to share trade secrets with another organization. In particular, there is little written guidance on protecting trade secrets before, during and after the period in which they are shared, leaving an opportunity to consider how best to approach intelligent sharing of one's valuable, secret information.

Typically, a trade secret owner will share a trade secret with another organization only in exchange for an acceptable commercial benefit. For example, such sharing might occur (1) between businesses engaging in due diligence[2] or otherwise exploring a potential relationship or engaging in an actual relationship, such as a license, collaboration or joint venture, or (2) between a business and a regulator, where the business is seeking approval or responding to a regulatory inquiry. Each scenario simultaneously raises confidentiality concerns or risks, which initially can arise in connection with sharing the trade secrets and subsequently can arise in connection with disentangling from, winding down or terminating any due diligence,

2. "Due diligence" can be defined as "research and analysis of a company or organization done in preparation for a business transaction." https://www.merriam-webster.com (accessed May 20, 2025).

exploration or relationship. Such subsequent concerns are akin to concerns that arise in connection with employee departures.[3]

Ultimately, balancing such benefit and risk is an important consideration when exploring, engaging in and, if or when necessary, disentangling from, winding down or terminating a relationship.

A key, but not unique, risk in business-to-business sharing is trade secret status can be lost if reasonable efforts or measures to maintain secrecy are not made. What can be unique in this commercial context is how to address that risk. Overall, due to tension between disclosure and protection, sharing should take place only after the disclosing party, e.g., the trade secret owner, secures suitable and verifiable protective efforts from the receiving party. Such efforts can be specified or embodied in contractual, physical or technological tools, or a combination thereof, that define, document and control the receiving party's acquisition, access, review, disclosure, use, protection, return and destruction (collectively, processing) of the trade secrets and corresponding materials, including documents and embodiments.

This Commentary addresses the risk-benefit balance by focusing on protecting trade secrets before, during and after sharing, while not unreasonably hampering either party's business operations or desire to engage in due diligence or a relationship. As noted above, such protection can be achieved through contractual, physical or technological tools. In more specific terms, those tools can include listing and identifying the trade secrets that are shared, designating specific individuals with whom the trade secrets are or can be shared, and specifying the purpose of

3. The Sedona Conference, *Commentary on Protecting Trade Secrets Throughout the Employment Life Cycle*, 23 SEDONA CONF. J. 807 (2022), substantively analyzes, for example, trade secret considerations that can arise in connection with employee departures.

the sharing, all of which would be part of the above-noted defining, documenting and controlling the receiving party's processing of the trade secrets and corresponding materials. This Commentary concludes with an Appendix which provides, in list form, some helpful questions for those disclosing to and those receiving trade secrets from a third-party organization.

Importantly, any such tools and, more broadly, any trade secret sharing, whether for commercial or regulatory purposes, will create an evidentiary record that may be part of subsequent litigation or arbitration involving one or more of the shared trade secrets. Such a possibility can inform choices about which tools to employ and how to employ them, bearing in mind that the use or omission of certain tools can impact the outcome of a litigation or arbitration.

The goal of the Commentary is twofold: (1) to identify potential issues when sharing trade secrets outside an organization and (2) to suggest pragmatic, potential solutions in light of marketplace reality. There is no one-size-fits-all approach for sharing trade secrets outside an organization, whether sharing trade secrets as standalone assets, or as assets that are part of a broader transaction. As such, the potential solutions, which are sometimes described herein as recommendations, are not intended to be and are not mandatory in any or every situation. Notably, artificial intelligence (AI) has a significant and growing role in the intellectual property arena. Regarding trade secrets, AI presents multiple opportunities and risks. An AI system, as well as one or more of its components, can be a trade secret, a tool or both. This Commentary addresses certain aspects of trade secret sharing where AI can be at issue in either or both capacities. As the relationship between AI and trade secrets evolves and the AI legal and regulatory landscape develops, updated or new commentary on these topics is expected. This Commentary does not address whether any specific tools,

protections, steps, measures or combination thereof constitutes reasonable efforts to maintain the secrecy of a trade secret because such a conclusion depends on the circumstances at issue and is a question of fact to be determined by a judge, jury or other fact finder.[4] This Commentary also does not address any domestic or foreign data privacy laws or regulations or how they might impact trade secret sharing within the United States or between the United States and a foreign country.

4. References in this *Commentary* to a "trade secret" are not meant to imply that a court or other authority, such as the U.S. International Trade Commission or an arbitrator, has concluded that the information is, in fact, a trade secret. Instead, a reference to a "trade secret" is a reference to an alleged or asserted trade secret. For more details regarding identification of trade secrets issues, *see* The Sedona Conference, *Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases*, 22 SEDONA CONF. J. 223 (2021).

II. REASONS FOR SHARING TRADE SECRETS WITH OTHER ORGANIZATIONS

Due diligence that includes sharing trade secrets typically involves uniquely situated parties and correspondingly unique challenges and risks. More specifically, the disclosing party and receiving party typically are organized differently and possess different types and amounts of resources. Their methods of operations, cultures, policies, procedures and levels of expertise with trade secrets and, on a higher level, with contract and information management also can vary. Such circumstances require deliberate discussion and, ultimately, tailored approaches to maintain the confidentiality of shared trade secrets.

In addition to each party's respective make-up, the contemplated and ultimate form of the parties' relationship informs the parties' approach during due diligence and beyond. For example, a joint venture or joint development work may require greater diligence before entering a formal relationship and more detailed, ongoing assessments of trade secret disclosure and use during the relationship than is typically required in connection with a narrower relationship, such as an investment in a start-up or a supply agreement. Further, if information, including trade secrets, is to be shared between competitors or potential competitors, then potential applicability of antitrust laws may need to be considered and certain guardrails, such as clean rooms, may need to be implemented to mitigate or avoid contamination or inappropriate sharing that might violate or lead to violation of those laws.[5]

5. For additional guidance about clean rooms, *see* The Sedona Conference, *Commentary on the Use of Clean Rooms*, 26 SEDONA CONF. J. 195 (2025), available at https://thesedonaconference.org/publication/Commentary_on_Use_of_Clean_Rooms.

The nature of a trade secret to be shared, including its value and form, also may inform the parties' discussion regarding an approach to protecting the trade secret. For example, the value of the trade secret to the disclosing party can, and often does, result in proportional levels of diligence and safeguards for that asset. As another example, where the trade secret is a single, i.e., the only prototype, the receiving party's access to the asset can and often will be in-person, site-specific and monitored.

Further, the parties often face time constraints. In other words, the parties may wish or need to quickly evaluate a potential business opportunity involving trade secrets. Such circumstances require balancing the time constraints with the need to protect the trade secrets. Trade secret owners who know what their trade secrets are and how they protect them are positioned to nimbly achieve that balance.

As to solutions, a confidentiality or non-disclosure agreement (NDA) is an example of a common tool used to protect trade secrets. Importantly, the rights, limitations and obligations set forth in an NDA, and in any broader agreement governing the parties' relationship, and the selection and tailoring of other tools used to protect trade secrets can be impacted by multiple factors.[6] Such factors include the parties' respective make-up, as noted above, the contemplated or ultimate form of the parties' relationship, the specific trade secrets at issue, the parties' past dealings with each other and their respective existing or potential third-party relationships, including a future merger, acquisition or sale of a party's business. Where the parties' overall relationship is defined in a written agreement broader than an

6. An NDA can be a stand-alone agreement, or it can be a portion of or provision within a broader agreement. For additional guidance about NDAs, *see* The Sedona Conference, *Commentary on Protecting Trade Secrets Throughout the Employment Life Cycle*, 23 SEDONA CONFERENCE J. 807 (2022).

NDA, such an agreement can set forth how, why, when, where and with whom trade secrets can be shared, and a protocol if the status, such as control, of either party changes during the term of such agreement. The agreement also may indicate what the trade secrets are by setting forth categories, or types, or general subject matter, of information. Setting forth categories of information does not mean identifying the trade secrets in the agreement. Rather, and for example, the agreement can cross-reference a securely stored addendum identifying or a secure depository for the trade secrets.[7]

Some common forms of relationships or contexts in which trade secrets may be shared include:

License: Generally speaking, a license is an agreement where the owner of certain subject matter, such as a trade secret, grants another individual or entity certain rights, such as the rights to access, disclose and use the trade secret.[8] Notably, the owner, i.e., licensor, retains ownership of, and corresponding rights to and interests in, the licensed subject matter, despite the grant of rights to the authorized party, i.e., licensee.

Licenses come in all shapes and sizes. They include various limitations, i.e., conditions or qualifications, such as: the duration of the license, bearing in mind that a license may be

7. Setting forth categories of information, as opposed to identifying trade secrets at issue, is an example of implementing the "need-to-know" practice to protect trade secrets. In other words, certain persons in the receiving party's operations who are responsible for business functions, including contract negotiation and management, may not need to know what the trade secrets are to fulfill their responsibilities.

8. *See* Defend Trade Secrets Act (DTSA), 18 U.S.C. § 1839(4) ("the term '<u>owner</u>', with respect to a <u>trade secret</u>, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the <u>trade secret</u> is reposed").

renewable and typically can be terminated, and that certain obligations, such as confidentiality obligations, may continue after a license expires or is terminated; authorization to use a trade secret for only a specific or limited purpose, such as to design, develop or sell a certain product or service, for only personal or commercial use or for use only in a specific field, market or geographic area; and the status of a licensee, such as a single, or exclusive, licensee or exclusivity in a certain product, service, field, market or geographical area.

Supply Relationship: In a supply relationship, a supplier, such as a vendor or independent contractor, provides goods, such as inputs, or services, such as fabrication of inputs, to a customer. Those goods or services may embody or have been produced with a trade secret—owned by the supplier or customer. Alternatively or additionally, a trade secret may be provided with a product or service to enable implementation or ensure compatibility with another product or service. These agreements are common in many industries and can play a major role in the functioning of national and global supply chains.

Supply agreements often include clauses addressing quantity, quality, product or service specifications, delivery time, cost of transportation and other parameters. Such a clause may constitute or include a trade secret. Additionally, where a supply agreement is part of or evolves into a longer term or ongoing relationship, the parties may enter a master service agreement (MSA). An MSA can include baseline provisions, including, for example, a baseline confidentiality provision, applicable to all or certain aspects of products and services.

Joint Venture, Joint Development or Other Collaboration: In some cases, a single company or individual may lack the expertise or resources to develop or bring to market a product or service. In these circumstances, two or more parties may enter a

business arrangement establishing a joint commercial enterprise where each party takes on specific responsibilities and corresponding costs and risks, and profits are apportioned. This type of arrangement is commonly referred to as a joint venture.

Joint ventures are common in many industries, such as the life sciences and pharmaceutical industries, and often involve research and development. For example, a company that has researched and developed science and technology around a device, diagnostic test or treatment may lack resources such as financial, human or manufacturing capital, capabilities, or expertise to seek and obtain regulatory approval for, or to develop, market and sell the device, test or treatment. That company may then form a joint venture with another company that can provide the necessary resources. Trade secrets may be shared and, in some situations, created as part of those joint efforts. Some or all of those trade secrets may constitute a capital contribution to the joint venture.

Sale of Goods or Services: A sale of goods or services is a basic and common transaction where one party, a seller, contracts with another party, a buyer, to transfer ownership of goods or render services in exchange for consideration. A supply relationship, which is discussed above, and a sale are separately mentioned because a supply relationship often involves providing inputs and a sale often involves providing the final or finished good or service.

Merger, Acquisition or Sale of All or Substantially All Assets: Mergers, acquisitions and sales of assets typically are transformative transactions. In a merger, one entity combines with another entity to create a new, singular entity. The new entity acquires all assets and liabilities of the absorbed entity. In an acquisition, one entity takes over another entity by purchasing all or most of the target entity's shares or other equity interests. In

a sale of all, substantially all or certain assets, one entity purchases specified assets and liabilities of a target entity.

Each type of transaction can present unique trade secret sharing issues. For context, each type of transaction may involve a transfer of trade secrets between the parties to the transaction or a continuation of, or a need to modify, previous or existing trade secret sharing between those parties or between a party to the transaction and a third party.

Notably, the ultimate consummation of such a transaction may not present the most significant, or any, trade secret sharing risks. Rather, due diligence preceding the transaction may present such risks. That is, depending on the particular transaction contemplated, a seller may share trade secrets with multiple prospective buyers. Such sharing needs to be handled carefully to ensure trade secret status is intact when only one buyer remains.

Investment, Including Securitization for Debt Financing: An entity or individual may acquire an interest in another entity in exchange for financial or another type of support. For example, a startup company may lack financial capital to develop, market or sell a product and, as a result, seek financing and possibly other capital, including human capital or expertise, from investors.

A common source of capital for founders of a startup who wish to retain an ownership interest in their company is venture capital (VC), private equity (PE) or both. In a typical investment model, a VC or PE firm will assess that opportunity through due diligence that includes evaluation of the startup's operations and assets, including trade secrets and other intellectual

property (IP).[9] If satisfied with that assessment, the firm may invest financial capital into the startup in exchange for an ownership interest in the startup. That is, the founders may sell all or part of their interests in the startup to the firm. The firm often gains a seat on or control of the startup's board of directors and, beyond the capital contribution, provides expertise to assist with the management and growth of the startup and commercialization of the startup's products or services.[10]

In another perhaps less common scenario, a startup may seek an infusion of financial capital through debt financing where it seeks to secure or collateralize the loan through certain assets, such as trade secrets. In such an arrangement, the trade secrets may be shared with the lender so the lender can perform its due diligence on, for example, the claimed status, i.e., confidentiality, and value of the pledged collateral.

Regulatory Approval: Advertising, marketing, selling or otherwise providing certain products or services to the public is regulated on many levels, ranging from international, national, state to local levels.

In the United States, regulators at the national level include the Department of Transportation (DOT), the Food and Drug Administration (FDA), the Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA). Assuming federal regulatory approval has been obtained

9. Trade secrets are not identified in any governmental grant or registration like patents, trademarks and copyrights are. Because of that lack of official documentation, evaluation of trade secrets often requires greater effort than evaluation of other IP. This *Commentary* is designed, in part, to facilitate that greater effort and, ultimately, sufficient evaluation of the trade secrets at issue.

10. Where a PE firm invests financial capital after a VC firm, the PE investment may replace or offset the VC investment.

for a product, service or facility, there also may be a need for state or local regulatory approval, such as with compounding pharmacies.[11]

While each regulator has its own specific process for applicants seeking and obtaining approval, a typical component of such a process is submission of sufficiently detailed information about the product or service at issue. Those submissions often are written. In certain circumstances, information also may be provided through an on-site inspection of a facility or operations. Such information can include, for example, safety and efficacy data from clinical or other trials or safety of a facility or operations. Notably, such information can include one or more trade secrets. Such inclusion is important because any information submitted or provided is at risk of public disclosure through the regulator's response to a Freedom of Information Act (FOIA), 5 U.S.C. § 552, request, a similar mechanism or otherwise. Indeed, that risk exists despite potential penalties for officers and employees of the United States and U.S. departments and agencies, such as the U.S. Department of Justice and Federal

11. Pursuant to section 503A of the Federal Food, Drug, and Cosmetic Act (FDCA), compounding pharmacies are allowed to provide drug products for patients whose clinical needs cannot be met by an FDA-approved drug product. Such pharmacies are exempt from certain sections of the FDCA, but only if the pharmacy is a State-licensed pharmacy. *See* U.S.C. §503A (exempting State-licensed pharmacies from § 501(a)(2)(B), which addresses current good manufacturing practice requirements, § 502(f)(1), which addresses labeling drugs with adequate directions for use, and § 505, which addresses approving drugs under new drug applications or abbreviated new drug applications). *See also* the Federal Trade Commission Act, 15 U.S.C. § 46(f) (addressing whether commercial or financial information obtained by the Federal Trade Commission can be maintained as confidential or privileged) *and* the Antitrust Civil Process Act, 15 U.S.C. §§ 1311-1314 (addressing potential exclusion of a Freedom of Information Act (FOIA), 5 U.S.C. § 552, request).

Trade Commission (FTC), who wrongfully disclose trade secrets.[12]

Additionally, existing and proposed laws and regulations impose or may impose record-keeping and disclosure obligations on developers and deployers of artificial intelligence (AI) systems. Such obligations can encompass, for example, technical information, such as training, testing and evaluation data, processes and results, as well as risks and realized harms, such as discrimination.[13] Such obligations seek to achieve, for example, transparency, traceability and explainability for AI

12. *See* 18 U.S.C. § 1905 ("Whoever, being an officer or employee of the United States or of any department or agency thereof, any person acting on behalf of the Federal Housing Finance Agency, or agent of the Department of Justice . . . , or being an employee of a private sector organization who is or was assigned to an agency . . ., publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets . . . of any person, firm, partnership, corporation, or association; shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.") and FOIA Exemption 4; *see also* 20 CFR § 402.90; and see, *e.g.*, Department of Justice Releases New Guidance on FOIA Exemption 4, The FOIA Ombudsman, available at https://foia.blogs.archives.gov/2019/10/21/department-of-justice-releases-new-guidance-on-foia-exemption-4/. For an example at the state level, see, *e.g.*, N.J.S.A. 47:1A-1.1, Government Records Exemption No. 6 ("Trade secrets and proprietary commercial or financial information obtained from any source. For the purposes of this paragraph, trade secrets shall include data processing software obtained by a public body under a licensing agreement which prohibits its disclosure"), available at https://www.nj.gov/dep/opra/exemptions.html.

13. *See, e.g.*, EU AI Act, Art. 53(1)(a) *and* Colorado (CO) AI Act, SB 24–205 §§ 6-1-1702-1704.

regulators, deployers and end users.[14] Importantly, trade secrets and other information may be excluded from disclosure obligations.[15] Whether or not such an exclusion applies, a receiving party may be obligated to maintain the confidentiality of disclosed trade secrets and other information.[16] In practice, the levels of record-keeping and disclosure required or deemed sufficient may vary by jurisdiction, i.e., by applicable legal and regulatory frameworks, and the particular circumstances at issue and likely will evolve over time. For a trade secret owner, a key takeaway or reminder is that the trade secret or confidential status of disclosed information can be eliminated or put at risk through disclosure. So, an informed and incremental approach to disclosure, especially with new and developing frameworks, can be a sound approach.

In some situations, persons subject to such laws and regulations will want to avoid needlessly eliminating or risking trade-secret status through excessive disclosure. So, a trade secret owner or holder may need or want to seek guidance or clarification from the corresponding regulator or other authority before or in connection with making any disclosure.[17]

---

14. *See, e.g., id.* and EU AI Act, Recital 27 ("Transparency means that AI systems are developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system, as well as duly informing deployers of the capabilities and limitations of that AI system and affected persons about their rights.")

15. CO AI Act, SB 24–205 §§ 6-1-1702(6), 6-1-1703(8).

16. *See, e.g.*, EU AI Act, Art. 53(7) and 78. See also note 8, *supra* (noting 18 U.S.C. § 1905).

17. Other situations where there may be a reason to share trade secrets with another organization include litigation finance and trade secret insurance transactions.

III. TOOLS AVAILABLE WHEN SHARING TRADE SECRETS

Parties who share trade secrets often proceed through a sequence of (1) pre-sharing, (2) sharing and (3) post-sharing. In other words, the sequence has three general periods: (1) the pre-due diligence or pre-relationship period (collectively, pre-sharing), (2) the due diligence or relationship period, (3) the post-due diligence or post-relationship period. Of course, due diligence may or may not result in a relationship and there may be a disentanglement or wind down before termination of the parties' interactions and commencement of the post-due diligence or post-relationship period.

Parties in a pre-sharing period may want to and perhaps should engage in high-level, exploratory discussions to determine whether deeper discussions, including sharing trade secrets, should proceed. Those exploratory discussions can focus on big-picture issues, such as contemplated forms of a relationship and the role of trade secrets in deeper discussions or a relationship. In turn, exploratory discussions may reveal obstacles that make actual due diligence or a relationship and initial or further trade secret sharing impractical or unappealing for commercial or other reasons. Notably, individuals engaging in exploratory discussions may not be and, in some cases, intentionally should not be the same individuals who will access, review and use shared trade secrets during due diligence or a relationship. In short, exploratory discussions can allow parties to walk away from a potential due diligence or relationship without having shared any trade secrets, or having shared only a high-level, non-confidential description of trade secrets, a representative trade secret or a limited number of trade secrets, thereby reducing, and perhaps eliminating, the risk of a subsequent trade secret dispute and related consequences.

If or when the parties decide to proceed with deeper discussions or to engage in due diligence or a relationship, there are three major categories of protective measures that a disclosing party may use to protect its trade secrets before, when and after the trade secrets are shared: (1) contractual tools, (2) physical tools, and (3) technological tools. Contractual tools, which are key administrative tools, can include NDAs and other agreements with confidentiality obligations, such as clean room or clean team agreements. Physical tools can include clean rooms for accessing and reviewing trade secrets.[18] Technological tools can include passwords and multi-factor authentication that restrict access to electronically or digitally stored trade secrets and enable monitoring of such access. Notably, training personnel is an overarching administrative tool that can be used to implement and bolster contractual, physical and technological tools. Indeed, training can foster a culture where trade-secret policies and procedures are understood and followed. Each category is further discussed below.[19]

Principle 1: Before and when trade secrets are shared, contractual tools, physical tools and technological tools can be used to protect the trade secrets and those tools can be

18. For additional guidance about clean rooms, *see* The Sedona Conference, *Commentary on the Use of Clean Rooms*, 26 SEDONA CONF. J. 195 (2025), available at https://thesedonaconference.org/publication/Commentary_on_Use_of_Clean_Rooms.

19. *See* SBS Worldwide, Inc. v. Potts, No. 13 C 6557, 2014 WL 499001, at *5 (N.D. Ill. Feb. 7, 2014) (plaintiff/ disclosing party adequately alleged it took reasonable measures to protect its trade secrets with a mixture of contractual, physical and technological tools).

supplemented, modified or enhanced throughout due diligence or a relationship.

IV. CONSIDERATIONS BEFORE DUE DILIGENCE OR A RELATIONSHIP

A. Personnel Involved

Principle 2: Sharing trade secrets calls for respective vigilance by designated personnel, such as a trade secret team, which may include a manager responsible for overseeing trade secret sharing, one or more individuals responsible for a certain aspect of that sharing, and in-house or outside counsel.

For a disclosing party, a starting point for sharing trade secrets with another organization can be assembling a team of individuals who will be engaged in sharing and protecting the trade secrets (Team). The Team members may be employees, agents or other representatives of the disclosing party. An in-house or outside counsel may be a Team member. The Team can focus on, for example, identification of the categories of information to be shared, the trade secrets to be shared, the selection and implementation of measures to protect the trade secrets and active monitoring of the receiving party's activities and compliance with its obligations.

Each Team member can be responsible for a specific area. Those areas can include: (1) project management, including communication and coordination with the receiving party, (2) subject matter expertise, i.e., knowledge of the trade secrets and any related information, to determine what can be shared or not, (3) legal expertise to identify the trade secrets and rights in and authorization to share the trade secrets, (4) security, including

physical or facility security, (5) data governance to account for applicable data policies and procedures, (6) information technology, including data management, to coordinate secure, electronic storage of and access to the trade secrets, (7) compliance, including the disclosing party's adherence to trade secret sharing protocols and the receiving party's implementation of protective measures, and (8) human resources to account for company policies and procedures relating to trade secrets. Each due diligence or relationship involving trade secret sharing is different, so a Team may include one or more of the foregoing or other individuals. For a small company, a Team may consist of only one individual or a few individuals responsible for fulfilling designated responsibilities. The volume and nature of the trade secrets, as well as the resources of a company, can also affect a Team's make-up. Where feasible, the Team should not comprise only lawyers. Non-lawyer Team members can provide unique, needed perspective and guidance during the sharing.

A receiving party can assemble its Team by accounting for the same or similar issues as the disclosing party, albeit from the opposite perspective. For example, one or more receiving party Team members presumably possess relevant, sufficient subject matter knowledge to assess the shared trade secrets and contemplated opportunity. Having said that, the receiving party may intentionally exclude from its Team one or more individuals who are integral to its operations. Such exclusion can avoid exposing those individuals to trade secrets and, as such, sufficiently preserve the receiving party's ability to continue, re-engage in or initiate its own pursuits if or when, for example, the parties' interactions end, or due diligence terminates. To facilitate such exclusion and related efforts, such as clean room management, the receiving party can internally identify its current or planned pursuits that sufficiently relate or may relate to the trade secrets. Overall, a receiving party Team will focus on

complying with applicable obligations, preventing missteps, such as inadvertently commingling disclosing party trade secrets with receiving party trade secrets or other information, and avoiding disputes relating to disclosing party trade secrets.

Notably, a disclosing party may request or require that a receiving party Team not include any individual who has worked with, is working with, or is expected to work with any existing or contemplated competing technology or subject matter, including any in-house or outside patent attorney or agent.[20] Such an exclusion can benefit both the disclosing party and receiving party by reducing the risk of a trade-secret misappropriation, breach of contract or other dispute.

Having said that, a receiving party may believe an exclusion will unduly inhibit its analysis and either (1) not agree to a requested or required exclusion, or (2) seek a narrower exclusion, such as an exclusion of any individual who has researched or developed, is researching or developing, or is expected to research or develop any existing or contemplated competing technology or subject matter. Before taking either of those positions, the receiving party should consider that an exclusion, and even a relatively broad exclusion, can be advantageous from an operational perspective. More specifically, an exclusion can avoid contamination of the receiving party's operations such that, if the parties' interaction is terminated, the receiving party can proceed with greater confidence that its pursuits will be uninterrupted by concerns of or actions by the disclosing party.

---

20. *See* Wellogix, Inc. v. Accenture, LLP, 823 F. Supp. 2d 555, 566 (S.D. Tex. 2011) (affirming jury's finding that the receiving party in a sharing relationship received trade secrets and was liable for trade secret misappropriation where it used this information in subsequent work for third parties), *aff'd sub nom.* Wellogix, Inc. v. Accenture, L.L.P., 716 F.3d 867 (5th Cir. 2013).

Where such an exclusion is not implemented, and the disclosing party is still willing to share its trade secrets, then modifications to the sharing process may be an option.[21] For example, the trade secrets may be shared in (a) sequenced fashion, i.e., trade secrets are gradually shared as opposed to all at once, or (b) segmented fashion, i.e., a part or parts of trade secrets are shared and then the complete trade secrets are shared if the parties decide to proceed with due diligence or a relationship.

If the disclosing party and receiving party are actual or potential competitors, then a data room, which may be or include a clean room, is an option to consider. Data rooms are further discussed below.

Team members should be contractually bound to protect any trade secrets disclosed or received. At least for the disclosing party Team, such contracts may exist prior to any sharing. If such a contract does not exist prior to any sharing, then the benefits of becoming a Team member may constitute sufficient consideration for a new or supplemented contractual obligation. A designated Team member or members can be responsible for ensuring proper contracts are in place and ensuring compliance with the contracts as a whole or with specific provisions, such as return or destruction of trade secrets. By obtaining copies of such executed contracts, the disclosing party can verify the receiving party has such contracts in place and confirm the roster of authorized individuals. The use of such contracts, or supplementation of existing contracts, in connection with the sharing is further discussed below.

---

21. In some situations, an exclusion may not be implemented because it is not feasible. A lack of feasibility may exist, for example, where a receiving party is a relatively small company with a correspondingly small group of employees.

Finally, some employers periodically train or at least remind employees about the value of, and obligations to protect trade secrets. Such efforts can account for applicable NDAs and other agreements. Similarly, the disclosing party and receiving party can agree to train or remind Team members and others involved in the trade secret sharing about their obligations relating to trade secrets in general, and the trade secrets to be shared. The frequency and extent of such training or reminding can be affected by the duration of the parties' interaction, due diligence or relationship.

B. Assets At Issue

> **Principle 3:** Trade secret sharing can be gradual, such that before trade secrets are shared, the parties can agree in writing on the types of trade secrets, by category, intended to be shared, and any such categories can be specific enough to make clear the types of information the receiving party will be obligated to protect.

1. Identification of Trade Secrets to Be Shared

Before any trade secrets are shared, the disclosing party can determine, perhaps in collaboration with the receiving party, the categories of information that the disclosing party will share and that the receiving party will need to evaluate or effectuate the potential or actual relationship. Designating and, if necessary, updating those categories can ensure that the disclosing party focuses its efforts and limits its disclosure and risks and that the receiving party likewise limits its risks. Disclosing no more than necessary and receiving no more than necessary are mutually compatible goals.

A disclosing party may be balancing two concerns when providing categories of information to the receiving party. On the one hand, categories should not be so detailed or specific that they reveal any trade secret. That is, absent appropriate protections, providing overly detailed categories can jeopardize trade secret status. On the other hand, categories that are too general may not provide the receiving party with an ability to sufficiently understand the actual or potential relationship, the relevance of the information already in its possession, which information may establish that a claimed trade secret is already known to it, or the expectations for or scope of protective measures.

In some cases, both the disclosing party and receiving party will know the categories of the information to be shared at the outset of their interactions. In other cases, there may be a need for collaboration between the parties following a high-level, initial disclosure. Ultimately, the disclosing party should describe the categories of information to be shared with enough specificity to make clear the types of information the receiving party will be obligated to protect throughout the due diligence or relationship so that proper safeguards can be agreed to and implemented.

A subsequent step for the disclosing party is to gather the information in those categories that will be shared. Within those categories, information may be (1) a trade secret, (2) confidential, sensitive or proprietary information that does not satisfy the legal definition of a trade secret, or (3) publicly or generally known information. A disclosing party's appreciation for, and proper accounting of, those different types of information is or can become important from an overall information governance or contract (e.g., license) management perspective, including where, as noted above, trade secrets and other information are submitted to a regulatory authority and non-trade secret

information is later sought through, for example, a FOIA request. Additionally, if information is publicly or generally known, then a disclosing party can share that information without protection and, as a result, potentially save time, money, and effort.

Once collected, a disclosing party should separate its trade secrets from the non-trade secret information so that the trade secrets can be readily tracked and, at the appropriate time, properly shared. Notably, this sharing may occur all at once, gradually or in stages. Such an approach can benefit both parties. A disclosing party that discloses fewer trade secrets, i.e., discloses only trade secrets needed to further the due diligence or other activity, exposes fewer trade secrets to risk of misappropriation or loss and can reduce expenditures of time, money and effort relating to, for example, protective tools. A receiving party that receives fewer trade secrets, i.e., receives only trade secrets needed to further the due diligence or other activity, reduces its liability exposure and likewise can reduce expenditure of time, money and effort relating to, for example, protective tools.

At this point, the disclosing party should: (1) know the categories of trade secrets that may be shared, and (2) be able to identify, and should internally identify, the trade secrets that may be shared.[22]

---

22. *See* Walmart Inc. v. Cuker Interactive, LLC, 2020 U.S. App. LEXIS 4289, **10–12 (8th Cir. Feb. 12, 2020) (a company's failure to clearly identify an alleged trade secret before its disclosure to a client precludes trade secret status); Health Care Facilities Partners, LLC v. Diamond, No. 5:21-CV-1070, 2023 WL 3847289, at *15 (N.D. Ohio June 5, 2023) (granting summary judgment in favor of defendant where, among other reasons, the disclosing party failed to identify its shared trade secrets during the relationship and to sufficiently protect them); and Scentsational Technologies, LLC v. PepsiCo, Inc., 13-cv-8645 (KBF), 2018 WL 2465370 (S.D.N.Y. May 23, 2018), *aff'd* 777 Fed.

A trade secret that is identified is set forth with sufficient particularity.[23] A prior *Commentary* addresses proper trade secret identification in litigation and the principles and guidance in that *Commentary* readily can be applied to trade secret identification in connection with due diligence or a relationship.[24] However, the context of due diligence or a relationship is different from the adversarial context of litigation. As such, the parties involved in due diligence or a relationship may agree to a less rigorous standard of sufficient particularity than would be required in misappropriation litigation.

Appx 607 (Fed. Cir. 2019) (trade secret claim fails without contemporaneous records describing the trade secret; such records were necessary to corroborate claim of joint creation of the trade secret).

23. A properly identified trade secret is a trade secret identified with sufficient particularity, and the identified trade secret is distinct from the categories of information eligible for trade secret status. *See, e.g.*, DTSA, 18 U.S.C. § 1839(3) (a "trade secret" is "all forms and types of financial, business, scientific, technical, economic, or engineering information," regardless of the medium of storage, compilation or memorialization if "(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information[.]"); *and* Uniform Trade Secrets Act (UTSA), §1(4) ("'Trade secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, 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, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."). The UTSA or a version thereof has been adopted by 49 States, and by the District of Columbia, with the only exception being New York.

24. *See* footnote 2, *supra*, referencing The Sedona Conference, *Commentary on Protecting Trade Secrets Throughout the Employment Life Cycle*, 23 SEDONA CONF. J. 807 (2022).

Once the disclosing party knows the categories of trade secrets and trade secrets that may be shared, it should account for its policies and procedures for identifying and protecting trade secrets, any applicable written agreements, such as NDAs, that protect trade secrets, any other contractual, physical or technological protective measures, or tools, such as marking, secure storage, segregation, limitations on acquisition, access, disclosure and use and any monitoring of the foregoing.[25] Where a disclosing party knows how it protects its trade secrets, it will be better able to determine and require appropriate, though perhaps not identical to its own, protective measures by a receiving party during due diligence or a relationship. Ultimately, protective measures taken by the disclosing party and the receiving party, respectively and collectively, need to satisfy the legal standard of reasonable measures.[26]

---

25. Examples of other contractual tools may include, to the extent enforceable, noncompete and non-solicit agreements.

26. *See* DTSA, 18 U.S.C. § 1839(3) *and* UTSA, § 1(4). Importantly, the reasonable protective measures requirement accounts for measures taken by a disclosing party, as well as measures taken by a receiving party. Geritrex Corp. v. Dermarite Indus., LLC, 910 F. Supp. 955, 961 (S.D.N.Y. 1996) ("Plaintiff must show that it took substantial measures to protect the secret nature of its information."); Big Vision Priv. Ltd. v. E.I. DuPont de Nemours & Co., 1 F. Supp. 3d 224, 267–69 (S.D.N.Y. 2014) ("There is virtually no contemporaneous documentary or testimonial evidence . . . indicating that Big Vision took *any steps* to ensure the confidentiality of the information it disclosed to third parties."); KT Grp. Ltd. v. NCR Corp., 2018 WL 11213091, at *13 (S.D.N.Y. Sept. 29, 2018) (citing Sw. Stainless, LP v. Sappington, 582 F.3d 1176, 1190 (10th Cir. 2009)) ("[D]isclosure of the alleged trade secrets to individuals or entities who are under no obligation to protect the confidentiality of the information extinguishes the owner's property right in the purported trade secrets."); *and* Nova Chems., Inc. v. Sekisui Plastics Co., 579 F.3d 319, 327–28 (3rd Cir. 2009) (holding that information disclosed to defendant distributor pursuant to a license "lost its trade secret status" because the license

Whether the protective measures taken in a situation will satisfy the reasonable measures standard is a question of fact decided on the totality of the circumstances, which may include standards applicable in the relevant industry, the value or importance of the particular trade secret at issue and the respective sizes and resources of the disclosing and receiving parties.[27]

Beyond satisfying the legal standard is marketplace reality. That is, a disclosing party may know, based on its own efforts, what physical and technological tools are effective. A disclosing party armed with that knowledge often wants a receiving party to implement the same, or substantially or sufficiently the same, tools as the disclosing party knows to be effective. Indeed, a difference between a disclosing party's tools and the receiving party's corresponding tools may make proving the existence of reasonable protective measures more difficult and may create exploitable or exploited risks that, in fact, lead to the misappropriation of the trade secret, corresponding operational and litigation expenses and corresponding injuries, including financial losses that may not be recoverable as part of any damages award.

2. Identification of What Is Not Part of Trade Secrets to Be Shared

Before any trade secrets are shared, the disclosing party also can identify information it will not share with the receiving party in connection with the evaluation or effectuation of the potential or actual relationship. The disclosing party simply may identify and not disclose certain information on its own.

---

agreement did not require defendant to "maintain the secrecy of any information it had acquired from [plaintiff]").

27. *See* The Sedona Conference, *Commentary on the Governance and Management of Trade Secrets*, 24 SEDONA CONF. J. 429 (2023).

Alternatively, the disclosing party and receiving party may collaboratively determine the categories of information that the disclosing party will not share with the receiving party. A contract provision authorizing a receiving party to reject receipt of information can also be employed. Such a provision can promote transparency in the information shared, encourage the receiving party to review the information shared, and limit or eliminate risks relating to information that the receiving party does not accept and, as required, returns or destroys. A contract provision authorizing the disclosing party to retrieve or claw back shared information likewise can be employed. In practice, such identification and determination and exercising of contractual provisions can avoid or enable correction of errors, such as inadvertent or excessive disclosure of information to the receiving party. But importantly, those steps are supplemental to a disclosing party monitoring the information it shares.

3. A Protocol for Potentially Sharing Additional Trade Secrets

As the evaluation or effectuation of the parties' potential or actual relationship unfolds, a need for the disclosing party to share additional trade secrets may develop. Alternatively or additionally, a need for the receiving party to share trade secrets may develop. Given those possibilities, the parties can agree to the circumstances and conditions under which the disclosing party can disclose additional trade secrets and under which the receiving party can become a disclosing party. While the terms of the parties' agreement may sufficiently account for such sharing, or certain aspects of such sharing, a substantive change to the evaluation or effectuation of the parties' potential or actual relationship, including any change in the scope of trade secret sharing or to a party's respective role as a disclosing or receiving

party, can lead to circumstances that warrant a review of and, as needed, revisions to the parties' existing agreement.

C. Protective Measures Before Sharing Trade Secrets

Principle 4: Where a party intends to share trade secrets with a receiving party, it can require the receiving party to implement initial protective measures, which are designed to be reasonable under the circumstances, before any trade secret is shared.

Sharing trade secrets with third parties increases the risk of, among other things, (1) misappropriation, i.e., unauthorized acquisition, disclosure or use of the trade secrets, and (2) loss of secrecy and, as such, loss of trade-secret status. An effective way to mitigate those risks is to implement protective measures before any trade secrets are shared and to be ready to timely enhance protective measures if sharing actually occurs.

As noted above, the three major categories of measures that a disclosing party may use to protect its trade secrets before, when and after the trade secrets are shared are: (1) contractual tools, (2) physical tools, and (3) technological tools. There is no one-size-fits-all approach to protective measures. Rather, those measures must be reasonable under the circumstances to establish and maintain trade secret status. Notably, establishing reasonable protective measures does not require implementing all the specific examples of protective measures discussed below. Moreover, none of the measures, alone or in any combination, are intended to reflect, establish or suggest any standard or industry practice at any stage of a trade secret sharing process.

1. Contractual Tools

A contract often is the starting point for protecting trade secrets before sharing them.

More specifically, parties contemplating trade secret sharing often enter into a confidentiality agreement, or NDA, that governs the acquisition, access, disclosure and use of the trade secrets and imposes additional protective measures, such as physical and technological tools, for the trade secrets.[28]

An NDA typically serves several important purposes. First, an NDA provides the receiving party with notice of the categories of information into which the disclosing party's trade secrets fall. Second, an NDA establishes the receiving party's contractual obligations to maintain the secrecy, or confidentiality, of the trade secrets and to refrain from acquiring, accessing, reviewing, disclosing or using the trade secrets in a manner not authorized by, or that exceeds the authorization provided in, the NDA.[29] Third, an NDA provides remedies to the disclosing

28. In practice, there may be differences between a confidentiality agreement and an NDA. However, in this *Commentary*, we treat the terms, i.e., agreements, as synonymous. An executed NDA often is the culmination of a drafting and negotiating process. The process typically commences when the disclosing party sends an NDA to the receiving party, with the hope that the receiving party simply will sign and return the NDA. That may happen where the disclosing party possesses greater bargaining power, including greater resources. A more typical scenario, however, especially between two similarly situated entities, is an NDA is executed after an exchange of revised drafts and negotiations. We raise this dynamic to illustrate there is no universally used NDA and, overall, each due diligence and relationship is unique. Accordingly, this *Commentary* is not meant to provide and does not provide a one-size-fits-all suggestion, recommendation, or requirement for an NDA or anything else.

29. If a dispute between the parties subsequently arises and litigation ensues, there may be an ancillary dispute over the terms of a corresponding

party if the receiving party breaches a contractual obligation. Fourth, an NDA is simultaneously an important protective measure and tangible evidence of reasonable protective measures, which must be taken for information to have trade-secret status.[30] Indeed, the absence of a written NDA when sharing a trade secret can make proving the existence of the trade secret, i.e., that reasonable measures were taken to protect the information at issue, more challenging and, ultimately, may eliminate a claim and remedies for trade-secret misappropriation.[31]

---

protective order. In particular, the parties may disagree over which, if any, individuals, other than outside counsel and retained, independent experts, are authorized to acquire, access, review, disclose or use asserted trade secrets or other confidential documents and information produced in discovery. Individuals so authorized under an NDA may be individuals that the parties wish to include, and can agree to include, as authorized individuals under the protective order. While actual or alleged conduct of an individual during or after the trade secret sharing process may weigh in favor or against such authorization under the protective order, the main point here is that individuals authorized under the NDA may provide a basis for resolving the ancillary dispute.

30. *See* note 7, *supra*.

31. *See, e.g.*, Abrasic 90 Inc. v. Weldcote Metals, Inc., 364 F. Supp. 3d 888, 898 (N.D. Ill. 2019) ("Failure to enter into nondisclosure or confidentiality agreements often dooms trade secret claims."). While not necessarily cast as such, an NDA is one of three common-sense, usually easily achievable protective measures that judges and juries readily understand and often expect to see. The other two common-sense, usually easily achievable protective measures are (1) marking as "trade secret," "secret" or "confidential" a document or file that is or includes a trade secret, thereby providing notice of the information's status to those who access it and (2) limiting trade secret acquisition, access, disclosure and use to those persons with a need to know the trade secret. Having said that, there is no mandatory protective measure(s) or tool(s) that must be implemented for information to have trade secret status.

An NDA is also like any other contract insofar as it may not address every issue that arises. For this reason, clear communication between the parties when negotiating an NDA is important. If documented and clear, communications between the parties may facilitate resolution of an issue relating to the NDA. Also, depending on the existence, validity and enforceability of an integration clause, those communications may be evidence in litigation or an alternative dispute resolution (ADR) process.[32]

Notably, an NDA can impact and be impacted by existing and future agreements, relationships and litigation involving the parties to the NDA or involving one or more of the parties to the NDA plus one or more third parties or former employees. As such, drafting, negotiating and complying with the NDA can involve each party accounting for and coordinating existing and anticipated obligations beyond the NDA. Such accounting and coordinating ideally takes place before the NDA is signed and any trade secret is shared because trade secret sharing, i.e., disclosure, can be the classic example of being unable to "un-ring" the bell, or requiring significant efforts to correct or limit actual and potential consequences. In short, an overall goal is to enter an NDA that is compatible with, and avoids a breach of or conflict with, relevant existing and anticipated agreements, relationships and litigation.

a. Definition of "Trade Secrets"

NDAs often define information being shared as "Confidential Information" and often include the term "trade secrets" within that definition. That approach may be convenient, but it often does not sufficiently focus the parties' attention on the

32. An integration clause is sometimes called a merger clause or entire agreement clause.

categories of trade secrets to be shared. Thus, parties who are about to share trade secrets should consider defining the term "trade secrets" in an NDA, and that is true even if they decide to define and account for "confidential information" and include "trade secrets" within the definition of "confidential information."[33]

Parties may have opposing views on how to define "trade secrets" in an NDA. For example, the disclosing party may want a broad definition of the categories to be shared, given that it wants to protect by contract as much of the shared information as possible. Conversely, the receiving party may want a narrow definition so that, for example, it is not broadly obligated or impaired or foreclosed from present or future activity in a certain field. Other times, both parties may want to narrowly define "trade secrets" so that the sharing is focused and notice regarding the respective rights and obligations is correspondingly clear. In other words, a focused definition should facilitate the disclosing party's efforts to collect and organize the trade secrets to be shared and result in the disclosure, receipt and management of fewer trade secrets. Where fewer trade secrets are at issue, the parties may save time, money and effort during the sharing and the overall risk, degree of potential harm and potential for a dispute may be reduced.

Notably, an NDA, like most contracts, typically provides a mechanism for the parties to amend a term or provision, such as

33. The definition of "trade secrets" addressed here is a subject matter definition where the categories of the trade secrets are described. The legal definition of "trade secret" is not being restated or otherwise modified. As discussed herein, the legal definition is being applied. The applicable legal definition, whether under the DTSA, a State's version of the UTSA or otherwise, can be accounted for in a choice of law provision within the NDA or would be determined during trade secret litigation or an ADR process.

the definition of "trade secrets." Bear in mind, however, that no matter what the definition of "trade secrets" is, or is amended to be, no trade secret should be identified in that definition or elsewhere in the NDA. Such identification should be avoided because it can risk unprotected exposure and loss of the trade secret. More specifically, a person who needs to acquire, access, review, disclose or use an NDA in connection with an administrative function, such as contract management, often does not need to know a trade secret. The definition of "trade secrets" also can include a procedural component. That is, a disclosing party typically is obligated to mark a shared trade secret in a particular manner so the disclosing party knows what trade secrets are disclosed and the receiving party knows what trade secrets it receives just by looking at the document or file.

An NDA also can exclude information from the definition of "trade secrets." For example, an NDA often states that "trade secrets" do not include information that is or becomes generally or publicly known through no fault of the receiving party.[34] However, if a trade secret becomes generally or publicly known, how that situation unfolded and who is at fault may not be clear.

One way for the disclosing party to potentially improve its ability to obtain relief under such circumstances is a provision where (1) the receiving party's specific protective measure obligations are listed and (2) the receiving party is obligated to protect the shared trade secrets with measures of protection that meet or exceed the measures it uses to protect its own trade secrets or, if it has no trade secrets, then its most important confidential information. The specific protective-measure obligations can provide a useful roadmap to investigate, determine and prove fault. So, too, can the protective measures used by the

34. *See, e.g.*, 18 U.S.C. § 1839(3)(B).

receiving party, especially if those measures likewise are listed in the NDA itself or set forth in an addendum to the NDA.

An NDA also can exclude from the definition of "trade secrets" information that was or is independently developed by the receiving party, i.e., developed without the use of the disclosing party's trade secrets, or previously known by the receiving party, i.e., known prior to the date the trade secrets were shared. *See, e.g.*, 18 U.S.C. § 1839(6)(B). Such an exclusion also may be supplemented by a corresponding provision specifying how, and possibly a date by which, a receiving party can or must claim that it previously independently developed or knew certain information.

Likewise, an NDA can exclude from the definition of "trade secrets" information that was or is reverse engineered by the receiving party. *See, e.g.,* 18 U.S.C. § 1839(6)(B). However, a disclosing party may need to carefully consider whether such an exclusion is tenable. For example, where a shared trade secret is a prototype, product, service, component or other item that is not commercially available, such an exclusion may unnecessarily provide an opportunity or defense for the receiving party.

The above discussion about the definition of "trade secrets" illustrates the need to carefully draft and review an NDA and tailor it to the specific circumstances at issue. This is not to say that certain terms or provisions, such as a provision for amending an NDA, may not be relatively standard or common. But accepting boilerplate terms or provisions, which may be presented as take it or leave it, can be costly.

Moreover, a failure to include any exception to or exclusion from the definition of "trade secrets" may erode the enforceability of the definition and, by extension, the NDA in any

litigation.[35] Taking into account the above discussion, an example of such an exception or exclusion is information that verifiably (1) was publicly or generally known prior to the sharing, (2) was known to the receiving party prior to the sharing, or (3) became known to the receiving party after the sharing, but not through a person who owed a duty of confidentiality to the disclosing party.

b. The Parties to the NDA

Another issue that often arises when negotiating an NDA is who—which entities and which individuals—will be parties to or otherwise bound by its terms. Where, for example, a transaction involves only two parties, i.e., one disclosing party and one receiving party, and each party is organized and operating in uncomplicated fashion, e.g., both are single-location companies with no affiliates, resolution of this issue can be relatively straightforward. However, where a transaction involves multiple parties organized and operating in complicated fashion, resolution of this issue can require greater inquiry and attention to detail and more specific NDA provisions. The parties can address, early in negotiations, their respective organizations and operations, including locations and affiliates, and which persons—e.g., affiliates, employees and other entities and individuals—will be parties to the NDA or otherwise bound by its terms. A person otherwise may be bound by, for example, a written, executed addendum to the NDA, a copy of which can be provided in timely fashion to the disclosing party. Where

35. *Cf.* Orca Communications Unlimited, LLC v. Noder, 314 P.3d 89, 94-95 (Ariz. App. Ct. 2013) ("The difficulty here is that the Agreement's definition of 'confidential information' extends far beyond the 'truly confidential.' . . . The definition's overbreadth makes the confidentiality covenant unenforceable.").

multiple jurisdictions are in play because the disclosing party and receiving party are located in different jurisdictions, or one of the parties operates in multiple jurisdictions, the parties can consider and address basic but important dispute resolution issues, such as choice of law and forum and venue selection.[36] To further illustrate the point, if an authorized affiliate or employee of the receiving party is in location X and another authorized affiliate or employee of the receiving party is in location Y, then the disclosing party can consider whether either location poses challenges that can be resolved or should be avoided. Those challenges may relate to enforcement of the NDA, or a certain provision, in a particular jurisdiction.

c. The Purpose for Sharing Trade Secrets

A key provision in an NDA is a provision that specifies the purpose for sharing trade secrets. Parties to an NDA often include a provision specifying the purpose for sharing trade secrets, stating the period during which the sharing can take place and limiting any acquisition, access, review, disclosure and use of shared trade secrets to the specific purpose. As discussed above, a typical purpose is to evaluate a potential future relationship between the parties, such as a license, sale of assets, merger or acquisition. Any acquisition, access, review, disclosure or use of a shared trade secret outside that purpose or for another purpose, such as advancing the receiving party's own commercial interests, can be prohibited. Also, the parties can include an NDA provision specifying the receiving party's receipt of and authorized activity relating to the shared trade secrets is not intended to create and does not create a commitment to enter a subsequent relationship with the disclosing party. Indeed,

36. These issues are further discussed below.

a receiving party may require such a provision because it is or may be assessing, or may want to maintain its ability to assess, one or more other relationships with persons other than the disclosing party. A disclosing party can assess whether such a requirement and any underlying circumstances can be adequately accounted for in the NDA and otherwise or whether the requirement and circumstances make sharing trade secrets with the receiving party too risky to proceed. An NDA provision that might address some of the disclosing party's concern and limit some of the risk is a provision specifying that the receiving party promptly notify the disclosing party, in writing, when it decides to end due diligence and not continue to a relationship with the disclosing party. Armed with that knowledge, the disclosing party can then take corresponding steps in timely fashion to protect its trade secrets and other interests.

d. Specifying Physical and Technological Tools

An NDA, i.e., a contractual tool, is typically not the exclusive means to protect shared trade secrets. Physical and technological tools, which are addressed in detail below, also are typically used. NDA provisions, or an addendum to the NDA, can specify the physical and technological tools to be used to protect shared trade secrets. Ultimately, those physical and technological tools complement, embody and implement NDA provisions relating to acquisition, access, review, disclosure, use and protection of shared trade secrets.

e. How Trade Secrets Can Be Acquired, Accessed, Reviewed, Disclosed and Used

An NDA also can set forth how the receiving party can acquire, access, review, disclose and use shared trade secrets. A provision addressing these issues can (1) set forth the points or locations and other details, such as channels and means, for

authorized individuals to acquire, access, review, disclose or use trade secrets and (2) describe or identify specific individuals authorized to acquire, access, review, disclose or use trade secrets. An NDA also may specify that individuals so authorized must verifiably acknowledge—e.g., in writing or by click—applicable obligations each time any such act occurs.

An NDA also can include a provision with additional prohibitions or limitations on when, where, why, how and by whom shared trade secrets may be acquired, accessed, reviewed, disclosed and used.[37] Typically, only an individual with a need to know a trade secret should be authorized to engage in any such activity. To that end, individuals, by name, title or category, with need-to-know status and such authority can be specified in an NDA, as suggested above, as can individuals, by name, title or category, who lack such status and authority.

f. Temporal or Durational Limitation on Confidentiality Obligations

An NDA may include a temporal restriction or durational limitation on confidentiality obligations, it may provide that those obligations continue so long as at least one shared trade secret remains secret, it may provide that those obligations continue on a per trade secret basis, i.e., with respect to a trade secret for so long as the trade secret remains secret, or it may provide that those obligations continue in perpetuity. Parties should be aware that some courts may view an NDA as a contract that can negatively impact competition and, as such, may

37. As discussed above, an NDA can include a provision stating the purpose for sharing trade secrets. The "why" here entails a provision that, for example, prohibits or further limits a specific individual's or specific individuals' acquisition, access, review, use and disclosure of trade secrets based on the timing or reason(s) for doing so.

look skeptically at a confidentiality obligation without a durational limitation.[38] Having said that, some trade secrets can exist forever, i.e., they can exist until they are no longer secret, other trade secrets may have a shelf life because once executed they become public—in the case of a marketing strategy, for example—and other trade secrets may, after a period of time, become stale and have no value—in the case of cost or pricing data, for example. A key point here is that any temporal restriction or durational limitation must be carefully assessed by both parties, and especially the disclosing party, as it can have a significant impact on trade secret status and the parties' respective rights and obligations. Evaluating the heft of obligations, if any, upon termination or expiration can be an important balancing exercise so as not to import too rigorous or too lenient conditions on protective trade secrets, particularly those that may undermine one's efforts to reasonably protect trade secrets.

g. Return or Destruction of Trade Secrets

An NDA can include a provision addressing how the termination of the parties' due diligence or relationship affects the NDA. The provision may state that confidentiality and other obligations continue, despite termination, and that the receiving party must take certain steps to protect shared trade secrets, including, for example, returning or destroying the trade secrets

38. *See, e.g.*, Carlson Grp., Inc. v. Davenport, No. 16-CV-10520, 2016 WL 7212522, at *5 (N.D. Ill. Dec. 13, 2016) (invalidating a nondisclosure clause as unreasonable and noting that the omission of a temporal limitation bears on its reasonableness.) *But see, e.g.*, 765 ILCS 1065/8 (b) ("This Act does not affect: (1) contractual remedies, whether or not based upon misappropriation of a trade secret, provided however, that a contractual or other duty to maintain secrecy or limit use of a trade secret shall not be deemed to be void or unenforceable solely for lack of durational or geographical limitation on the duty").

in its possession, custody or control. Importantly, an NDA can include a provision requiring the receiving party to acknowledge, in a signed writing, the specific trade secrets returned or destroyed and that no copy of, and no file or document containing, based on or derived from, any trade secret has been retained. As a practical matter, a return or destruction obligation is an obligation of which the disclosing party can affirmatively remind the receiving party once the due diligence or relationship is terminated. Also, an NDA may set forth exclusions to the return or destruction obligation, such as: (1) documents or information that must be retained by the receiving party in order to comply with an applicable legal or regulatory obligation, with such return or destruction promptly occurring upon termination of the legal or regulatory obligation, (2) document or information back-ups in the ordinary course that are not accessible by any unauthorized person, where such back-ups will be destroyed, or permanently deleted, in the normal course of the receiving party's document retention or destruction policy, a copy of which the receiving party has provided to the disclosing party for further, calendared follow-up, for example, (3) where a dispute between the parties exists, documents or information relating to, or that reasonably may relate to, the dispute may be retained by the receiving party's outside counsel until the dispute is fully and finally resolved, after which return or destruction promptly occurs or further retention is subject to conditions set forth in, for example, a protective order or settlement agreement, and (4) limited C-suite-level or Board-level documents or information, such as meeting minutes, with any such documents and information subject to corresponding protective measures, including limited access and redaction obligations, and destroyed, or permanently deleted, in the normal course of the receiving party's document retention or destruction policy, a copy of which the receiving party has provided to

the disclosing party for further, calendared follow-up, for example.

Further, proper return or destruction of trade secrets can be undermined where the event triggering the return or destruction and the date by which to do so is not clearly set forth in the NDA. Specifying an event, such as written notice or a due diligence or relationship milestone, is one way to specify a triggering event and the corresponding date for return or destruction.

h. Remedies

An NDA can specify remedies for a breach of the NDA. Relatedly, an NDA can include three provisions that impact the availability of those remedies: (1) a pre-litigation dispute process; (2) choice of law; and (3) selection of forum and venue.

Pursuant to a pre-litigation dispute provision, the parties may be required to attempt to resolve any dispute, such as a claimed breach, prior to commencing litigation or other dispute resolution processes.[39] While each situation is unique, a disclosing party may be hesitant to agree to a time-consuming or involved pre-litigation dispute process, especially considering the relative fragility of trade secrets.[40] Indeed, even where an NDA includes a pre-litigation dispute provision, a disclosing party often will seek a provision that allows it, at any time, to seek a temporary restraining order and preliminary injunction for

39. For example, a disclosing party may claim that a receiving party breached an NDA by failing to comply with a protective measure requirement, such as a requirement to implement a specific contractual, technological or physical tool. The NDA may specify a notice, inspection and cure process for the claimed breach, consequences for the claimed breach if not cured and remedies for a breach proven in litigation.

40. Kinship Partners, Inc. v. Embark Veterinary, Inc., 3:21-cv-01631-HZ, at *17 (D. Or. Jan. 3, 2022) ("A trade secret once lost is, of course, lost forever.")

actual or threatened misappropriation. In contrast, a receiving party may be content with a pre-litigation dispute provision that requires relatively involved efforts to resolve any dispute prior to commencing litigation.

Pursuant to a choice of law provision, the parties can specify the State law that will govern the interpretation and enforcement of the contract and the law that will govern a trade secret claim or issue. An informed choice of law decision will account for the validity and enforceability of NDA provisions under the chosen law. As discussed above, some courts applying some States' laws may scrutinize and limit an NDA because of anti-competitive effects, just as those courts would scrutinize, for example, a noncompete or non-solicitation agreement or provision (noncompetes and nonsolicits). The same can be said for an ADR forum, such as an arbitrator, a panel of arbitrators or a mediator. A trade secret claim may be brought under federal law, i.e., the Defend Trade Secrets Act, 18 U.S.C. § 1836 (DTSA), or state law, i.e., a State's version of the Uniform Trade Secrets Act (UTSA) or New York common law. A trade-secret claim generally comprises the same or similar elements under the DTSA, UTSA and New York law, although interpretation and application of those elements can differ according to the jurisdiction. Certain claims, such as inevitable misappropriation, are available only under certain trade secret laws. Certain remedies may be available under only federal or a certain State's trade secret law. Extraterritorial application of the law at issue can also vary and factor in the choice of law decision.

With respect to a forum and venue-selection clause, the primary issue is whether a court, including a jury, or an ADR forum, will hear and decide a dispute. A forum and venue-selection clause often mandates a single forum and venue for any dispute between the parties that arises out of or relates to the

NDA.[41] ADR may be an attractive process for the receiving party because a claimed breach of the NDA, i.e., alleged bad acts, may be addressed in a confidential environment, such as arbitration, instead of in a publicly accessible courtroom and on a publicly accessible docket.[42] An arbitrator also may be less likely than a court to award injunctive relief. ADR may be an attractive process for the disclosing party because a confidential environment, such as arbitration, can make it easier to maintain the secrecy of an asserted trade secret. At the same time, the disclosing party may want a judge and jury to hear and decide its misappropriation case, with such a desire potentially more pronounced where substantial damages, enhanced damages or attorneys' fees are or may be in play. Of course, depending on the goals, circumstances and experience of each respective party and the nature of the interaction or transaction at issue, a given party's preference for a certain forum, venue and process may, at the time the NDA is entered, run counter to those general propositions. Another factor to consider is a party's familiarity with a particular forum, venue and process, and the forum's or venue's overall experience and body of case law relating to trade secret misappropriation. Finally, where the parties are domiciled and, in particular, the locations from which they operate also may

41. *See* Paragon Micro, Inc. v. Bundy, 22 F. Supp. 3d 880, 891 (N.D. Ill. 2014) (compelling trade secret misappropriation case to arbitration), *citing* Shearson/American Exp., Inc. v. McMahon, 482 U.S. 220, 226, 107 S. Ct. 2332, 96 L.Ed.2d 185 (1987) ("This duty to enforce arbitration agreements is not diminished when a party bound by an agreement raises a claim founded on statutory rights.").

42. The arbitrability of a dispute—that is, whether a dispute is encompassed by an ADR clause—can be the subject of costly litigation before an arbitrator, court or both. So, if ADR is the parties' desired dispute resolution process, then clear, express terms about which disputes are to be so resolved should be used.

factor in reaching an agreement on a forum and venue selection clause. One party may not wish to litigate a misappropriation case on the so-called "home court" of the other party, where the jury's and perhaps even the judge's familiarity with a party may create a home-court advantage. At the same time, the other party may wish to litigate a misappropriation case where, for example, certain witnesses and a physical facility are located.

i. Other Documents, Including Other Agreements

In addition to an NDA, there are other documents that may be negotiated and exchanged between parties prior to sharing trade secrets. These documents may include (a) policies and procedures for employees of, or other individuals affiliated with, the receiving party who are authorized to acquire, access, review, disclose or use shared trade secrets and (b) as discussed above, acknowledgments, signed by those employees or other individuals, in which they acknowledge and agree to be bound by the NDA and accompanying policies and procedures.

The parties also may enter into agreements that protect against unfair competition, such as noncompetes or non-solicits. Noncompetes may proscribe the receiving party from engaging in certain competitive activity or lines of business while it possesses or can acquire, access, review, disclose or use the disclosing party's trade secrets, and for a period thereafter, which period may be based on or a proxy for an independent development period. Notably, if there is a dispute, the receiving party may argue that such a period is the maximum duration of any injunctive relief the disclosing party can seek and obtain.[43]

43. "[T]he most commonly employed standard [for calculating the duration of an injunction in a trade secret case is]: 'the period of time that would be required for independent development'" of the trade secret. ShowCoat Sols., LLC v. Butler, no. 01:18-cv-789-ALB, *11 (M.D. Ala. Mar. 19, 2020)

Non-solicits may proscribe the receiving party, or both parties from, for example, soliciting and hiring key employees of the other party for a certain period.[44] Key employees authorized to acquire, access, review, disclose or use shared trade secrets also may enter noncompetes or non-solicits.

Notably, noncompetes and, relatedly, NDAs and non-solicits have been and are subject to increasing attention from, for example, Congress, the FTC, the National Labor Relations Board and certain State legislatures. That attention has resulted in state laws and proposed federal laws and regulations restricting, or, in some situations, banning noncompetes. Further, other agreements, such as NDAs and non-solicits, may be within the scope of some of those restrictions and bans, meaning that those other agreements may be challenged and invalidated or rendered unenforceable as overly broad. As such, parties should account for applicable, enacted laws and regulations and case law when it comes to noncompetes and other, related agreements. Additionally, non-solicits may raise antitrust or other competition considerations. Parties likewise should account for those considerations.

(internal citation omitted). While the independent development period is sometimes referred to as the head-start period, the term head-start period is often used to identify the period within which a "[d]efendant's misappropriation gave it a leg up on the competition" and, as such, the period within which a plaintiff is entitled to damages. AMS Sensors U.S. Inc. v. Renesas Elecs. Am. Inc., no. 4:08-cv-00451, *11 (E.D. Tex. Feb. 26, 2021) (internal citations omitted).

44. A non-solicit may be an agreement directed to certain customers, employees or a combination of those persons and prohibits a party to the agreement from, for example, soliciting those customers, employees or a combination of those persons. A non-hire, or non-poach, agreement may be an agreement directed to certain employees and prohibits a party to the agreement from, for example, soliciting and hiring certain employees.

2. Physical Tools

Physical tools are tangible, often readily visible measures, such as notices and barriers, for protecting trade secrets. A disclosing party, such as a trade secret owner, often uses physical tools to protect its trade secrets. At the pre-due diligence or pre-relationship stage, the disclosing party will not likely share identified trade secrets. So, at this pre-sharing stage, physical tools that the receiving party will be required to use during due diligence or a relationship—when the receiving party acquires, accesses, reviews, discloses and uses shared trade secrets—can be investigated and assessed and then specified in the NDA. Such physical tools can include the disclosing party's physical tools the receiving party will likewise need to maintain or implement. Such communication and, ultimately, cooperation can reduce the risk of physical tool deficiencies, mistakes, or failures, which can negatively impact an asset's trade secret status. In some situations, the disclosing party may want the rights to inspect, approve and require supplementation or modification of the receiving party's physical tools to further reduce that risk and avoid any misunderstanding, ambiguity or conflict.

There are multiple physical tools available. Physical tools can be promulgated through contractual or other administrative tools, such as trade secret policies and procedures. Training new or returning employees on those policies and procedures, including periodic refresher training and updated training, is an example of another administrative tool.

The use of any physical tool depends on the circumstances at issue and there often is a relation or overlap between contractual, physical and technological tools.[45] For example, an NDA

45. Protective measures, i.e., all contractual, physical and technological tools, typically are considered together in assessing whether the measures

may require that the paper version of the document be marked as "Trade Secret" or "Confidential" and the same information in electronic form, i.e., electronically stored information (ESI), be digitally marked in the same manner. Likewise, where an NDA may require that a document be stored in a locked room or safe, the paper version of the document may be stored in a locked room or safe, and the same ESI may be password-protected, encrypted and stored on a local hard drive in a locked room. Examples of physical tools used to protect trade secrets include:

---

have been and are reasonable. *See* Hertz v. Luzenac Group, 576 F.3d 1103, 1113 (10th Cir. 2009) (noting that "Luzenac took a series of steps to protect the secrecy" of its process and "there always are more security precautions that can be taken. Just because there is something else that Luzenac *could* have done does not mean that their efforts were unreasonable under the circumstances[;]" and holding that "whether precautions were, in fact, reasonable, will have to be decided by a jury") (emphasis in original); Surgidev Corp. v. Eye Tech., Inc., 828 F.2d 452, 455 (8th Cir. 1987) (explaining that "[o]nly reasonable efforts, *not all conceivable efforts*, are required to protect the confidentiality of putative trade secrets") (emphasis added); TouchPoint Solutions, Inc. v. Eastman Kodak Co., 345 F. Supp. 2d 23, 30-31 (D. Mass. 2004) ("But the standard is reasonableness, not perfection. . . . the [Confidential Disclosure Agreement's (CDA)] existence is some evidence of reasonable security measures. . . TouchPoint also put into place numerous other security measures. . . Kodak's response, that compliance or non-compliance with the CDA is dispositive of the reasonableness of security measures, would render the taking of all other precautions pointless. That is not the intent of the preferred inquiry."). Having said that, particular tools, i.e., one or more contractual, physical or technological tools, can be evaluated for reasonableness. Where trade secrets are to be shared, an evaluation of overall or particular tools can include the disclosing party's tools and the receiving party's tools. *See*, *e.g.*, *TouchPoint*, 345 F. Supp. 2d at 30 ("even with a written CDA in place, the Court may examine the conduct of the parties to determine the scope of their confidential relationship and the reasonableness of their efforts to protect secrecy.")

- Labeling, Printing and Copying
    - Mark trade secrets with express, conspicuous labels, watermarks or legends, such as "Trade Secret" or "Confidential"
    - Use tracking devices or indicia
    - If printing or copying is allowed, print, or copy trade secrets on copy-proof or non-photocopiable paper
    - Use color-coded paper to identify a document containing a trade secret or a specific-colored paper for a specific document containing information at a certain level of confidentiality
- Facility and Transport Security
    - Secure trade secrets in one or more of: locked drawers, filing cabinets, safes, or rooms
    - Mark areas containing trade secrets as "confidential," or with a similar designation
    - Control and restrict access to those marked areas
    - Store trade secrets in a secure area, such as an office or other room with a door, rather than a cubicle or open space
        - Maintain trade secrets in windowless rooms
        - Provide secure work areas where trade secrets can be acquired, accessed, reviewed, disclosed and used without exposure to others who are not authorized to engage in any such activity
        - Maintain access logs for anyone entering a secure area where trade secrets are

stored, acquired, accessed, reviewed, disclosed, used, embodied, or in operation

- Require key card or code access for employees and other authorized individuals, including levels of permission, especially for secure areas
- Install gated, perimeter fences to keep out uninvited, unscheduled, or uncontrolled visitors
- Install video surveillance cameras to monitor ingress to and egress from the facility, building, or secure area, such as where trade secrets are stored, acquired, accessed, reviewed, disclosed, used, embodied or in operation
- Install alarm systems
- Install bars on windows
- Employ security guards to verify visitors through, for example, photo identification, and to log and admit visitors at facility, building, or secure-area entrances
- Employ security guards and dogs to patrol the grounds during and after business hours
- Transport trade secrets via secure carriers and in locked, secure containers

- Visitor Protocols
  - Maintain logs of visitor entry and exit
  - Require visitors to be identified and badged when on premises
  - Require visitors to sign agreements not to acquire, access, review, disclose, use or remove any company information without permission

- Escort visitors while in the facility, building or secure area
- Search visitor bags when entering and exiting the facility, building, or secure area
- Prohibit recording of any audio and video and taking of any photographs during visits by, e.g., collecting devices with any recording capability, such as a camera, and affixing security tape to cover any camera lens

- Employee Obligations
  - Employee manuals, policies and guidelines for trade secrets, in printed or ESI form, distributed to employees who sign and date acknowledgments of receiving, reading, and understanding those materials. Such materials can include corresponding explanations of:
    - What trade secrets are, such as by categories of information, and how they are marked and protected and
    - Who can, i.e., is authorized to acquire, access, review, disclose, or use trade secrets, with whom they can discuss and to whom they can disclose trade secrets, and to what extent and under what circumstances or conditions such discussions and disclosures can occur
  - Treatment of a third party's trade secrets, including segregation from the company's trade secrets
  - Instructions on storage of trade secrets, including securely storing lab notebooks in, for

example, a locked area or desk and password protecting e-lab notebooks, and not leaving the lab notebook unattended in an area or on a desk or opened on an unattended laptop, tablet or other device

- Travel protocols, such as using privacy screens on approved or issued travel devices, including laptops and tablets, not leaving any devices unattended or unsecured, and not taking trade secrets with you, whether on a laptop, tablet, or other device
- Protocols for the return or destruction by, for example, shredding or deleting, of any embodiment or copy of a trade secret where the embodiment or copy is no longer needed, the need to know the trade secret ceases or the authority to access the trade secret is terminated, including upon employment termination or furlough, whether voluntary or involuntary
- Protocols for securing a trade secret when off-site, including when at home, working remotely or traveling, if off-site trade secret access or related activity is authorized by, for example, securing it in a locked office or filing cabinet or on a password-protected, authorized laptop, tablet, or other device and in a password-protected file
- Incident response plan to address actual, potential, or suspected trade secret misappropriation, including any unauthorized acquisition, access, review, disclosure or use or related activity, events or issues

- Obligations under and responsibilities and roles in an incident response plan, including procedures for timely reporting any actual, potential, or suspected (i) breach of a policy or procedure for protecting trade secrets or (ii) unauthorized acquisition, access, review, disclosure, or use of a trade secret
- Initial, refresher, and updated training sessions for new, returning, and existing employees[46]

3. Technological Tools

A disclosing party often uses technological tools to protect its trade secrets. As with physical tools, technological tools can be promulgated through administrative tools, such as policies and procedures, including employee training. At the pre-due diligence or pre-relationship stage, the disclosing party will not

46. *See, e.g.*, MicroStrategy Inc. v. Business Objects, S.A., 331 F. Supp. 2d 396, 403, 420 (E.D. Va. 2004) (finding MicroStrategy "took reasonable steps to preserve the secrecy of its information" by having, among other things, "physical security, such as locked doors, limited access to its buildings through the use of badges, and the use of security cameras"); U.S. v. Shanshan Du, 570 Fed. Appx. 490, 500 (6th Cir. 2014) (reasonable measures included physical security such as "a locked facility monitored at all times by security guards, who required employees to show a photo identification to enter . . . guards checked all bags and computer devices carried out of the building, patrolled the facility after hours, and escorted visitors within the facility"); U.S. v. Hanjuan Jin, 883 F. Supp. 2d 977, 998-99, 1008 (N.D. Ill. 2012) (reasonable measures included security officers, cameras, alarms and gated car access with key card); Smithfield Packaged Meats Sales Corp. v. Dietz & Watson, Inc., 452 F. Supp. 3d 843, 858 (reasonable measures included physical security such as "codes, badges, or fobs to access its physical offices and plants, and requir[ing] visitors to sign agreements preventing them from removing information from offices and plants").

likely share its trade secrets. So, at this stage, technological tools that a receiving party will use during due diligence or a relationship—when the receiving party acquires, accesses, reviews, discloses or uses shared trade secrets—can be investigated and assessed and then specified in an NDA. Such technological tools can include the disclosing party's technological tools that the receiving party will likewise need to maintain or implement. Such communication and, ultimately, cooperation can reduce the risk of technological tool deficiencies, mistakes or failures, which can negatively impact an asset's secret status. In some situations, the disclosing party may want the right to inspect, approve and require supplementation or modification of the receiving party's technological tools to further reduce that risk and avoid any misunderstanding, ambiguity or conflict.

Importantly, contemplated or actual use of technological tools can create the impression that the disclosing party agrees to electronically share all the trade secrets to be shared. In fact, a disclosing party may agree to share one or more trade secrets, initially or thereafter, only in physical or paper form and only in a secure physical location where contractual and physical tools are utilized. Under such circumstances, the use of technological tools may not be necessary.

The disclosing party should be well prepared, based on its own operations and technological tools, to specify the technological tools the receiving party needs to maintain, implement, supplement, or modify. Indeed, in the modern, remote world, trade secrets often are electronically created, stored, acquired, accessed, reviewed, disclosed and used by the disclosing party.[47] That electronic activity occurs on and through a variety

47. Trade secrets that are electronically created, stored, acquired, accessed, reviewed, disclosed and used by the disclosing party also are subject to technological threats.

of systems, equipment, devices and media, such as proprietary databases, shared folders and drives, cloud systems, email and other communication platforms, portals, such as VPNs, on-site computers and remote computers, including laptops, tablets and smartphones. The disclosing party's awareness of its trade secret-related electronic activity, systems, equipment, devices and media, as well as the corresponding technological tools it utilizes, should significantly inform its technological tool requirements for the receiving party.

For example, the disclosing party may have to decide whether to provide the receiving party access to its platform or portions thereof. If such access is provided, then the disclosing party can determine the credentials needed to gain access and the manner in which, including the device or devices through which, access will be permitted. Where appropriate and possible, the disclosing party also can test or conduct a dry run of, or periodically audit or evaluate, the access protocol to ensure it functions properly and to identify and troubleshoot vulnerabilities or risks, including those that may have been unanticipated or overlooked.

Overall, the disclosing party can keep in mind four important platform-related issues: (1) whether the platform is sufficiently secure, such that trade secrets can be shared with tolerable or minimal risk of misappropriation by unauthorized persons, whether affiliated with the receiving party or not; (2) whether the platform is configured to allow access to trade secrets on only a need-to-know basis, i.e., to only authorized individuals;[48] (3) whether the platform is configured to allow access

48. Failing to limit trade secret access to only those individuals who need to know the trade secrets in connection with the due diligence or relationship can be evidence that the trade secrets were not reasonably protected. *Cf.* George S. May Int'l Co. v. Int'l Profit Assocs., 256 Ill. App. 3d 779, 783, 628

on only certain days and at only certain times; and (4) whether the platform is configured to monitor who accessed what trade secrets, when and by what means and to monitor other activity, such as downloading and printing, assuming such other activities, or functions, are enabled and permitted.[49] Addressing those issues before sharing trade secrets can help ensure that those measures properly are in place and operational when the trade secret sharing takes place.

Importantly, the disclosing party can consider and address essentially the same above four issues if it will be establishing a data or due diligence room—including one that is or includes a clean room—for trade secret sharing. Such rooms are further discussed below.

There are multiple technological tools that the disclosing party can use to protect trade secrets or, if segmented, portions of trade secrets, that are in electronic or digital form. Some of those tools can be used, or inform the tools to use, when protecting shared trade secrets. Examples of those tools include:

- Password Protection and Encryption
    - Password-protect documents, files, folders, and devices that are or contain trade secrets
    - Require complex passwords with frequent change intervals and password storage protocols, including storage in physically secured drawers or encrypted virtual password lockers

N.E.2d 647, 650 (1st Dist. 1993) (holding that information was not a trade secret where it was disclosed without a confidentiality agreement to employees of plaintiff, which experienced a turnover of 600 employees annually); *see also* UTSA, §1, comment.

49. Such monitoring may produce key evidence in a subsequent trade secret misappropriation, breach of contract or other dispute.

  - Use two- or multi-factor authentication technologies for trade-secret access
  - Encrypt at rest and in transit: encrypt documents, files, and folders that are or contain trade secrets when they are stored and if they are transmitted, and encrypt devices, hard drives and memory devices on or in which a trade secret is stored
- Activity Tracking
  - Maintain computer logs that track trade secret access by, for example, a trade secret identifier, such as a sequential number that does not disclose the trade secret, the name of the accessing person, and the date and time of platform, network, folder, file log in/log out, and access to/access out
  - Maintain computer logs tracking the device used to access a trade secret
  - Maintain computer logs of any trade secret downloading, uploading, copying, printing, attaching, emailing, including forwarding, saving/saving as, revising or deleting, bearing in mind that all such functionality often can be permanently disabled
  - Generate alerts on detection of any, or an abnormal volume or timing of, trade secret downloading, uploading, copying, printing, attaching, emailing, including forwarding, saving/saving as, revising or deleting, optionally with threshold generating interruptions of acquisition, access, review, disclosure and use of a trade secret

- Limiting Access
    - Limit remote access to the computer network, platform, folders or files that are or contain a trade secret
    - Allow access to a trade secret only from authorized devices, such as company-issued desktops, laptops and tablets
    - "Fingerprint" files that are or contain a trade secret with a marker, such as a typographical error or other benign error or content, to more easily prove trade secret misappropriation or breach of contract if that ever becomes necessary
    - Disable data ports on computers to prevent downloading or uploading trade secrets onto a remote memory device or other memory or storage medium
    - Adopt cyber-security protocols
        - Quarantine excessive or suspicious email traffic
        - Limit or prevent access to social media accounts
        - Limit or prevent access to certain websites
        - Install and update malware and anti-virus software
        - Include, in an incident response plan, a response to any intrusion attempt or cyberattack, including individuals' responsibilities and roles and steps to be taken

- Secure and verifiably erase trade secrets in electronic, digital, or magnetic memory after need for that copy has ended or memory is replaced or redeployed
- Maintain trade secrets on computers or servers electronically, but physically disconnect the computers or servers from internal or external networks, including any WIFI or internet connection or access
- Limit source-code sharing to secure, third-party escrow services that have proper access controls and limit or prohibit any downloading, uploading, copying, and printing of that code
- Ensure vendors and other business partners implement and comply with protective measures[50]

V. CONSIDERATIONS WHEN SHARING DURING DUE DILIGENCE OR A RELATIONSHIP

A. Identify Assets at Issue

Principle 5*:* Sharing trade secrets is an attentive process where a disclosing party identifies a trade secret when it is shared and the disclosing

50. *Cf.* Arkeyo, LW v. Cummins Allison Corp., 342 F. Supp. 3d 622, 630-32 (E.D. Pa. 2017) (no trade secrets in source code that plaintiff published on the internet for fifteen months without employing standard industry protections, e.g., there was no encryption, password protection, code obfuscation or confidentiality provisions or requirements that users abide by any terms; court observed that "Arkeyo committed the cyber equivalent of leaving its software on a park bench.").

party and receiving party protect the shared trade secret.[51]

Principle 6: Sharing trade secrets is an attentive process where a disclosing party, on its own or in collaboration with a receiving party, can provide and update categories of to-be-shared or shared trade secrets, identify additional shared trade secrets, specify shared trade secrets returned or destroyed by the receiving party and specify and update entities and individuals who are or are not authorized to acquire, access, review, disclose or use the shared trade secrets.

Issue No. 1: If a trade secret is not properly identified when it is shared, then potential consequences are:

(a) The trade secret—i.e., subject of the disclosing party's and receiving party's protective efforts—may not legally exist and trade secret status may be lost;

(b) The receiving party lacks notice of the trade secret requiring protection, thereby resulting in compromised secrecy and potential loss of trade secret status;

(c) An inaccurate valuation of the trade secret and, as a result, a lower economic return on the trade secret;

(d) Less control over, and reduced ability to track, the receiving party's acquisition, access, review, disclosure and use of or

51. The Sedona Conference, *Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases*, 22 SEDONA CONF. J. 223 (2021), substantively analyzes the standard for proper trade secret identification, i.e., sufficient particularity, and provides examples of proper trade secret identification.

to the trade secret, and post-due diligence or post-relationship, return or destruction of the trade secret;

(e) Inadvertent sharing of other information, including other trade secrets. In other words, a disclosing party should not disclose more than necessary, and a receiving party likewise should not want to receive more than necessary. Corresponding, respective concerns include loss of trade-secrecy status for inadvertently disclosed trade secrets and potential exposure to claims that were not contemplated;

(f) Difficulty in identifying, or failing to identify, joint developments or modifications and corresponding rights and interests;

(g) Difficulty in pursuing a trade-secret misappropriation claim against the receiving party or a third party; and

(h) Increased difficulty in proving, by clear and convincing evidence, a prior commercial use defense under 35 U.S.C. § 273 and, in particular, the subject matter to which the defense applies.

The identification process can include the receiving party identifying its related or similar trade secrets, communicating and verifying that it possessed a disclosed trade secret prior to disclosure and separating pre-existing or ongoing work from the parties' relationship.

The receiving party also can confirm the disclosing party's measures to protect the shared trade secrets and prevent transfer of any trade secret rights, whether outright or through derivative works, to another person.

1. Identification Of Trade Secrets Shared

The transition to due diligence or a relationship typically warrants a correspondingly heightened protocol for sharing trade secrets, i.e., a stricter protocol than may have been used

for pre-due diligence or pre-relationship sharing of a list of categories of the trade secrets. In other words, trade secrets likely were not and, absent reasonable measures to protect the trade secrets, should not have been shared before due diligence or a relationship. During due diligence or a relationship, trade secrets will be shared, and corresponding identification obligations of the disclosing party and confidentiality obligations of the receiving party will need to be fulfilled for the due diligence or relationship to proceed.

Once due diligence or a relationship commences, existing obligations set forth in a prior agreement, such as an NDA, may not cease. Rather, all or some obligations may continue, to the extent sufficient and applicable, or they may be supplemented, modified or enhanced while accounting for the parties' focus on the commercial objectives of the due diligence or relationship and recognizing that a transaction, for example, may or may not come to fruition, change, evolve or terminate. Obligations may continue, for example, where a triggering event or condition in a prior agreement occurs or is satisfied. Obligations may be supplemented, modified or enhanced in a new agreement or in an addendum to a prior agreement.

As noted in Section IV, there are three major categories of protective measures for trade secrets before, during and after due diligence or a relationship: (1) contractual tools, (2) physical tools, and (3) technological tools, as well as corresponding administrative tools, such as employee education and training. Trade secret owners should consider utilizing all three types of tools when protecting trade secrets during due diligence or a relationship. While tools can be organized into those three categories for ease of discussion, the different tools are, in practice, connected.

At the inception of due diligence, a disclosing party should possess a list of identified trade secrets it intends to share and know the tools that have been or will be implemented by the receiving party to protect the trade secrets. To be clear, a due diligence or relationship list of trade secrets can include the identified trade secrets, and that contrasts with a pre-due diligence or pre-relationship list of categories of trade secrets, which should not include the identified trade secrets. Alternatively, the identified trade secrets may be an addendum to the due diligence or relationship trade-secret list, with such an approach potentially facilitating more controlled disclosure of the shared trade secrets by the disclosing party and more controlled acquisition, access, review, disclosure and use of or to the shared trade secrets by the receiving party.

Additionally, a disclosing party should be mindful of contexts in which disclosure of trade secrets is occurring to consider whether they are consistent with the agreed-upon categories. If the parties have not previously agreed in writing on a category into which a to-be-disclosed or disclosed trade secret falls, then previously agreed to categories can be supplemented prior to disclosing the trade secret or upon realizing that the disclosed trade secret lacks a corresponding category. Such supplementation of categories can help to ensure accurate accounting of shared trade secrets.

Principle 7: Sharing trade secrets is an attentive process that can be part of a disclosing party's or receiving party's broader information governance and management process, where tools that a receiving party is to use to

> protect trade secrets can be specified in a contract, such as an NDA.

As noted above, a common starting point, or first tool, for protecting trade secrets during due diligence or a relationship is a contract, such as an NDA, that limits acquisition, access, review, disclosure and use of or to trade secrets. During due diligence or a relationship, the parties may enter an NDA that continues, modifies or builds upon an existing NDA or another agreement. Notably, an NDA used in connection with due diligence typically will limit such trade secret activities to only evaluation of a possible future relationship. Further, an NDA used in connection with due diligence or a relationship may account for supplemental, modified or enhanced physical and technological tools to protect trade secrets shared during due diligence or a relationship.

The NDA often addresses both written and oral sharing, i.e., disclosure of trade secrets. Oral sharing may occur during, for example, an interview, meeting or demonstration relating to due diligence or a relationship. Such sharing typically can be memorialized through a procedure in the NDA that allows post-sharing written identification of trade secrets. Other oral sharing may occur outside a scheduled interview or meeting. For example, a receiving party may seek, and a disclosing party may provide extemporaneous supplemental or clarifying information because of human error, i.e., a trade secret may have been insufficiently identified when initially shared. Regardless of the circumstances, any oral sharing may be subject to differing interpretations or recollections. So, as a general proposition, oral sharing often is not preferred. But if it does occur, it can be promptly and accurately memorialized in writing pursuant to the agreed upon procedure.

Pursuant to the NDA, progressive, incremental sharing can be an appropriate approach. Under this approach, trade secret sharing will be gradual and contained. For example, (1) only trade secrets in a certain category or categories initially will be shared, (2) only a representative trade secret or representative trade secrets in each category initially will be shared, (3) only a very limited number of persons initially will be authorized to acquire, access, review, disclose and use the trade secrets, and (4) time constraints will be placed on stages of acquisition, access, review, disclosure, use and, ultimately, evaluation of the disclosed trade secrets. Then, if there is mutual interest in continuing the process towards, for example, a relationship—the sharing— including the number of authorized persons and duration of authorization, can incrementally progress. Notably, progressive, incremental sharing can allow parties to more easily terminate the due diligence and part ways.

Confidentiality obligations in an NDA often are mutual. That two-way street accounts for a common dynamic of information sharing. Specifically, during due diligence or a relationship, a disclosing party often becomes a receiving party and vice versa. For example, the receiving party, prior to receipt of a trade secret from the disclosing party, may have conducted its own research or development relating to information it receives. To establish its rights and interests, the receiving party will share its information with the disclosing party. The receiving party also may have third-party obligations that require it to obtain mutual confidentiality obligations. Thus, while due diligence or a relationship initially may focus on rights and obligations that protect a disclosing party's trade secrets, there often is a need for corresponding rights and obligations to protect the receiving party's trade secrets, and sometimes a third party's

trade secrets, that also are shared during the due diligence or relationship.[52]

Mutual sharing of trade secrets or related information also may occur—and corresponding protections are therefore appropriate—where new trade secrets may be jointly developed or existing trade secrets may be modified. Notably, confidentiality obligations relating to shared, jointly developed or modified trade secrets can continue where due diligence ends without a subsequent relationship, such as a licensor-licensee relationship, or where the subsequent relationship terminates.

Unsurprisingly, a receiving party often seeks to limit the duration of confidentiality obligations and, in effect, put a shelf-life on the trade secrets at issue. Such limitations typically conflict with the desire of a disclosing party. The disclosing party often wants confidentiality obligations to continue in perpetuity or until the trade secret becomes generally or publicly known through no fault of the receiving party. Sometimes there is room for compromise as to certain trade secrets. For example, a trade secret may have a natural shelf life because it will be publicly or generally known when executed (e.g., a marketing plan) or comprises data (e.g., cost or pricing data) that is time-sensitive, meaning data that loses its value or becomes stale as time passes and market conditions change. Additionally, the parties may agree to treat trade secrets differently than other confidential information when it comes to the duration of confidentiality obligations.

---

52. *See* Edifecs Inc. v. TIBCO Software, 756 F. Supp.2d 1313 (W.D. Wash. 2010). *Cf. Big Vision Private Ltd v. E.I. DuPont de Nemours & Co.*, 1 F. Supp.3d 224 (S.D.N.Y. 2014), *aff'd* 610 Fed. Appx. 69 (2nd Cir. 2015) (trade secret owner unable to enforce alleged trade secrets because it failed to give potential joint venturer, who also had been developing technology in the same area, clear notice of trade secrets shared).

During due diligence, information frequently is shared through a data room. Depending on the limitations on access to the room and the information stored in the room, a data room can be or include a clean room. Whether one is considering a physical, i.e., in-person, virtual, i.e., remote, or combined physical and remote data room, trade secrets in the data room can be protected (1) with the tools addressed in Section IV.C. above and (2) by requiring that persons authorized to access the data room and acquire, access, review, disclose or use the trade secrets not be involved in certain activities, such as research, development, engineering or patent prosecution, or with certain products or services, such as existing or planned competitive products or services.[53]

2. Identification of Trade Secrets or Other Assets Modified or Jointly Developed

Principle 8*:* Sharing trade secrets can lead to the generation of additional, protectible assets, such as modifications to or derivations from those trade secrets and jointly developed trade secrets, the identification of and rights to which the parties can address in writing.

Where trade secrets are shared, related research, development and engineering efforts may take place. Sometimes those efforts are joint efforts and sometimes those efforts are parallel, independent, supplementary or complementary. A result of

53. For additional guidance about Clean Rooms, *see* The Sedona Conference, *Commentary on the Use of Clean Rooms*, 26 SEDONA CONF. J. 195 (2025), available at https://thesedonaconference.org/publication/Commentary_on_Use_of_Clean_Rooms.

those efforts can be modifications, including improvements, to shared trade secrets, derivations from shared trade secrets and jointly developed, new assets, including trade secrets, all of which are topics that can be addressed in an agreement that governs the parties' relationship.

Also, just as pre-due diligence or pre-relationship protective measures, or tools, can be supplemented or enhanced as the parties transition into due diligence, such supplementation or enhancement can occur as the parties transition into a post-due diligence relationship. In other words, mutual and respective measures in effect during due diligence or pre-relationship often can continue, with appropriate modifications, into the relationship. The need for such continuation, with modifications, can be attributable to the parties' evolving interactions. Due diligence generally includes a sharing model comprising disclosure of trade secrets by the disclosing party, acquisition, access, review, disclosure and use of or to the trade secrets by the receiving party and discussions between the parties. In contrast, development work during a relationship typically is a more interactive process, with suggestions and collaboration that build on the parties' preceding activity.

A key issue to address when it comes to modifications to or derivations from a trade secret is who owns the modified or derived subject matter, whether jointly developed or not. Parties can agree to joint ownership, where each party owns an undivided interest in the subsequently developed asset, with the right to sub-license. Another option is sole ownership by one party, with a license to the other party. The parties also may agree, as part of such an arrangement, that, if or while owner/licensor status is unresolved, each party shall have certain rights, such as a right to use the subsequently developed subject matter under certain conditions and for a certain term. The receiving party also may seek a feedback or residuals clause in the NDA

or a related agreement. Under a feedback clause, the receiving party obtains, for example, a right to use, or even own, the feedback it provides to the disclosing party if the feedback modifies or improves the shared trade secret or other information, products, services or processes. Under a residuals clause, the receiving party has, for example, a right to use information, namely, general knowledge, that it received if such information is retained through unaided memory. The important point here is to timely contemplate and, if appropriate, timely address the issue of what rights, if any, attach to the fruits of the labor attendant to the sharing of trade secrets. A failure to do so can result in an avoidable and costly situation, including litigation or another dispute resolution process.

An important step in assessing whether subject matter is a subsequently developed asset is a complete and accurate list and identification of the trade secrets that each party has shared with the other party. Likewise, listing and identifying what is not being shared or included in a relationship can be important, especially if the parties' relationship, and corresponding agreements, have evolved from, for example, pre-due diligence to due diligence to post-due diligence relationship.

Additionally, there can be disclosure obligations where the party first aware of the subsequently developed asset discloses it to the other party. Such an obligation can be buttressed with corresponding audit and inspection rights, or even a portion of an incident response plan addressing steps to be taken where there is non-compliance or reason to believe there is non-compliance with applicable obligations.

In addition to defining ownership, control and maintenance of subsequently developed trade secrets and other assets, parties can specify in a joint development (or other agreement) other aspects of their relationship, such as the corresponding

royalties or other compensation that will be due, the availability of and procedures for exercising audit and inspection rights, the effects of a change in ownership or control of either or both parties, and the reasons for and consequences of termination of the agreement or overall relationship. Parties also can specify which party, or parties, may apply for, own and enforce specific assets, such as patents, and cooperation or other obligations in connection with the application process and enforcement actions.[54]

Finer points for which the parties can account include timely documentation of trade secrets or other information each party has or has not contributed to a modified, derived or jointly developed trade secret or other asset and when any such contribution occurred. Timely documentation of a contribution can facilitate progress of ongoing development work, often is important to establish legal rights and interests in and to the results of development work and can avoid, or reduce the time and expense of, a dispute that may develop between the parties. To those ends, parties can update the list and identification of trade secrets shared, as well as prepare and update a list of modified, derived or jointly developed trade secrets or other assets, as the relationship proceeds. Procedures for such updates, or preparation and updates, including timing and related audits and inspections, can be accounted for in a joint development or other agreement, and corresponding governance, compliance or oversight liaisons or committees may be part of such procedures. Compliance with such procedures can be a precondition to bringing or defending an action against the other party.

54. *See*, *e.g.*, Lucent Techs., Inc. v. Gateway, Inc., 543 F.3d 710 (Fed. Cir. 2008)

B. Updating Protective Measures When Sharing Trade Secrets

As the relationship between the parties evolves, it may become necessary to update the contractual tools to protect shared trade secrets and other assets. Depending on the rigidity or flexibility of the contractual tools in place, such updated, i.e., supplemental, modified or enhanced, tools may be necessary to accommodate, for example, ownership or license rights to modified, derived or jointly developed trade secrets or other assets, including tangible assets and other intellectual property. As a more specific example, negotiation or renegotiation of a residuals clause, or a ban or limitation on a party's future acquisition, access, disclosure and use of or to such trade secrets or other assets may be needed.

Also of note are the broader issues of compliance with contractual obligations and exercising contractual rights as the relationship evolves. For example, there may be an increase, a plateau or decrease of trade secrets being shared, with each such scenario presenting the parties an opportunity to assess whether obligations have been met and are still applicable and adequate, i.e., whether they need to be updated to account for changed circumstances, and whether rights have been timely and properly exercised and are still adequate. Such obligations may include sales reporting and royalty payment obligations for commercial use or embodiments of a trade secret. Such rights may include audit and inspection rights. Those rights may include the right to audit which personnel, such as key individuals, are still, no longer or newly involved in the relationship and if not, why and if so, how. Also, use of a third-party neutral to assess compliance with one or more obligations may be an appropriate process for the parties to consider and include in their relationship at a certain point, if such a process was not initially or is not yet part of their relationship. Likewise, it may become

necessary to update the physical and technological tools to protect shared and other trade secrets, i.e., any modified, derived or jointly developed trade secrets.

Common physical tools, as discussed above in Section IV.C.2, control access to the shared trade secrets. A notable example of such a tool is a data room for evaluating shared trade secrets. Examples of related technological tools are software to log who accesses a physical data room, such as with a key card or biometric information, and software to log who accesses ESI through a device in that room or through a device that provides access to a virtual data room. Updating such physical and technological tools often depends on an assessment of the personnel accessing the data room and the cards, information and devices being used to gain access to the data room and trade secrets. Typical inquiries include whether such devices are authorized, accounted for, being used properly and running current versions of software. Issues that may be identified include unauthorized downloading, uploading, copying, attaching, saving or printing of trade secrets. Such activities would likely result in updating corresponding physical and technological tools to meet the agreed level of protection and possibly result in taking other steps to protect and enforce respective interests and rights.

VI. CONSIDERATIONS WHEN ENDING DUE DILIGENCE OR A RELATIONSHIP

When due diligence or a relationship ends, measures to protect the confidentiality and thus, the status and value of a shared trade secret are typically taken. Some of those measures may continue beyond the due diligence or relationship and some may be supplemental, modified or enhanced measures that commence when the due diligence or relationship ends. Those measures may be set forth in an NDA or other contract between the disclosing party and receiving party. Generally, both parties

will have protective measures obligations, with the disclosing party often focused on the receiving party's compliance with its obligations. That focus often includes the disclosing party seeking confirmation, in action and writing, that the receiving party has met and will continue to meet its obligations. For example, and as discussed above, the disclosing party often will expect and seek (1) return or destruction of the shared trade secrets in the receiving party's possession and (2) the receiving party's written confirmation that those obligations have been fulfilled. A receiving party also often has one or more continuing obligations, such as an obligation to maintain the confidentiality of the trade secrets it received and an obligation to refrain from accessing, reviewing, disclosing or using them. That obligation can be part of a belt-and-suspenders approach that accounts for the possibility of the receiving party breaching or otherwise failing to comply with the return or destruction obligation, whether by refusal, deficiency, mistake or otherwise.

Depending on how the trade secrets were shared and the obligations specified in the NDA or other contract, a disclosing party may also expect and seek written verification that: (1) any devices, platforms, databases or repositories, which the disclosing party provided or to which the disclosing party provided access, are returned or disabled, (2) any information, which the disclosing party provided or to which the disclosing party provided access and which was or is stored on any device the receiving party will continue to possess is deleted, and (3) the receiving party reminds its team members and others involved in the trade secret sharing of confidentiality obligations. Permanent deletion of trade secrets may be achievable, especially if the receiving party adhered to obligations regarding, i.e., limitations on storage, acquisition, access, review, disclosure, and use of or to the trade secrets. At the same time, the parties may agree that the receiving party can maintain in confidence and securely

store archival copies that can be acquired, accessed, reviewed, disclosed, or used only during or in specific circumstances, such as a dispute concerning the trade secrets. Those archival copies may be maintained by and stored with, for example, an outside attorney, an in-house legal department, or an approved third party.

A disclosing party should account for any written materials, physical materials, such as a prototype or model, and digital or physical credentials, such as usernames, passwords, key cards or badges, that were provided to the receiving party and ensure they are returned, destroyed or disabled**.** To bolster protective measures and possibly motivate compliance and reduce the risk of a breach or other failure by the receiving party, whether by refusal, deficiency, mistake or otherwise, a disclosing party also can provide written reminders to the receiving party of its continuing obligations, including confidentiality obligations. A disclosing party also can compare the most current list, or inventory, of disclosed trade secrets to a list, or inventory, of returned or destroyed trade secrets to further those same purposes.[55] This comparison can be quite important, as it objectively determines which trade secrets may be at risk, or at a higher risk, of misappropriation. Depending on the terms of the NDA or other contract, other measures, such as interviewing receiving party personnel about awareness of and compliance with obligations and potential risks, also can be taken. Notably, such measures are an example of measures that may be seen as not commercially feasible or reasonable, especially by the receiving party. Indeed, such a viewpoint may exist when the NDA or other contract is

55. The information set forth in both lists should be enough for the list to serve its purpose, with the disclosing party or both parties evaluating the scope of information and level of detail according to the contractual terms of their relationship.

being negotiated or when the disclosing party requests such measures without a contractual basis for doing so.

Because of the prevalence of ESI, human error and sometimes even bad intent, the return or destruction of all relevant information may not be possible. But as noted above, a disclosing party can still compare the trade-secret inventories and, if necessary and accounted for in the NDA or other contract, inventory and examine relevant devices, including forensically. Devices that can store trade secrets include smart phones, computers, whether a desktop, laptop or tablet, external storage or memory devices and any online accounts provided to or accessed or used by the receiving party. Whether a given device is or was an authorized device is also an important issue. As such, timely preparing and updating an inventory of authorized devices is a step the disclosing party can take, preferably in cooperation with the receiving party, to assist in the return or destruction process. The disclosing party can also compare the returned information to the tracked history of the receiving party's information access and, as appropriate, act upon any discrepancy.

The above measures, along with the discussion below, provide a framework for a disclosing party to protect its trade secrets when and after a due diligence or relationship ends, whether by its own terms or by termination. A receiving party can also consider this framework as a possible means to facilitate its compliance with obligations and reduce its risk of committing trade secret misappropriation or breaching an NDA or other contract.

As noted above, an NDA, like any contract, may not address every issue that arises. In other words, circumstances can be overlooked or unforeseen during a contracting process. Nevertheless, many parties can negotiate and agree to provisions that

will provide more certainty and better protection—for the trade secrets and the parties—when ending the due diligence, as always happens, or ending the relationship, as often happens. Below, we discuss several issues of which parties should be aware when ending due diligence or a relationship and potential ways to address those issues.

Principle 9: The ending of due diligence or a relationship where trade secrets were shared is an opportunity for the parties to confirm, in writing, the status of the sharing, including the trade secrets that were shared and the receiving party's return or destruction of the shared trade secrets and other materials, such as documents identifying or embodiments of the shared trade secrets.

A. Failure to Update and Finalize Identification and a List of Trade Secrets Shared, Modified or Jointly Developed

A disclosing party is responsible for knowing what its trade secrets are, properly identifying and listing them, and updating and finalizing such efforts when sharing them with a receiving party. Thus, at or near the conclusion of due diligence or a relationship, the disclosing party should know what trade secrets were shared and be prepared to confirm that sharing, in writing, with the receiving party. In other words, this confirmation process, which can be set forth in an NDA or another contract between the parties, is an opportunity to align the parties' understandings regarding the trade secrets shared and any rights and obligations relating thereto.

There may be a legitimate, objective dispute about what trade secrets were shared or the parties' current situation may not be amicable, and communication may not be timely, clear or

sufficient. One way to potentially avoid or limit those or similar circumstances is for the NDA or other contract to set forth a process for providing or obtaining confirmation or clarification of the identification or list of the shared trade secrets. Such a process could be in effect throughout the trade secret-sharing process. If it is, then the process might encourage greater attention to detail by each party and might lead to more productive communication, whether the parties' situation is amicable or not. Whether such a process is in place or not, when the identification or list of shared trade secrets is or may be open to interpretation, either party can proactively confirm or clarify or seek confirmation or clarification of the identification or list of the shared trade secrets. If any such effort is made, it can, ideally, be made in writing. Such effort can reduce the risk of and perhaps eliminate a future dispute, or at least reveal a current dispute.

Such a process is not without potential pitfalls. If the receiving party does not seek confirmation or clarification and a future dispute arises, such a failure may expose the receiving party to corresponding liability, or greater liability, or waive or otherwise negatively impact its rights or defenses.[56] Depending on the terms of the process, the disclosing party may or may not be obligated to confirm or clarify the identification or list of the shared trade secrets upon request of the receiving party. But the failure to do so may waive or otherwise negatively impact the disclosing party's attempt to subsequently do so in litigation.

Also worth mentioning is a late request for confirmation or clarification where a process for doing so is not set forth in the NDA or other agreement. That is, if the receiving party makes such a request at the end or nearly the end of the parties'

56. Convolve, Inc. v. Compaq Computer Corp., 527 Fed. App'x. 910 (Fed. Cir. 2013) (failing to comply with NDA's written follow-up memoranda requirements waived party's rights under the NDA).

relationship, then it may trigger scrutiny from the disclosing party, result in greater overall uncertainty for the receiving party and, in the event of litigation, a stronger argument from the disclosing party that the receiving party waived or limited its rights or defenses. This situation especially illustrates the potential benefits of greater attention to detail during the trade secret-sharing process and, where appropriate, timely requests for confirmation or clarification pursuant to an NDA or other agreement or even in the absence of an express contractual provision.

A trade secret may be deliberately modified during the parties' due diligence or relationship. In other words, the trade secret may be modified not because of a deficiency or error, but to account for a different component, input, interface or application, for example. Three issues immediately can arise, and those issues can be addressed in the NDA or another agreement between the parties. First, are the modifications—including who made the modification, the date of the modification and other pertinent details—properly and timely documented? Second, who owns the stand-alone modification, i.e., potential trade secret, and corresponding rights and interests? Third, who owns the modified trade secret, i.e., the original trade secret plus the modification, and corresponding rights and interests?

Finally, the parties may be in a joint venture or other joint development-based relationship, or joint development may occur as the parties' relationship progresses or evolves. The parties, through their efforts, may jointly develop assets, including potential trade secrets, and one or both parties may then derive assets from a jointly developed asset. Like the circumstances where a modified trade secret is at issue, three issues immediately can arise, and those issues can be addressed in the NDA or another agreement between the parties. First, is the joint development work—including who performed the work, the date of the work and other pertinent details—properly and timely

documented? Second, who owns the jointly developed asset and corresponding rights and interests, including the rights and interests in any derivative assets? Third, if only one party owns the jointly developed asset and corresponding rights and interests, does the other party retain or receive any rights or interests, such as a non-exclusive right or license to use the jointly developed asset?

B. Trade Secrets Not Returned or Destroyed When Due Diligence or a Relationship Ends

The parties' NDA or other contract can include a provision obligating the receiving party (1) to return or destroy all the trade secrets it received, (2) to do so upon the disclosing party's written request or fulfillment of another condition, such as the ending of the parties' due diligence or relationship, (3) to do so by a certain deadline, and (4) to confirm, in writing, to the disclosing party that all such trade secrets have been returned or destroyed. In many situations, the receiving party can satisfy those obligations. Indeed, with notice of those obligations in an NDA, i.e., before any trade secrets are shared, the receiving party can take steps to ensure its means and scope of acquisition, access, review, disclosure, and use of the shared trade secrets will not interfere with—and will facilitate—those obligations.

Even with those obligations in place, a receiving party may fail to return or destroy all received trade secrets when due diligence or a relationship ends. Such a failure may result, for example, from (1) a receiving party's deliberate decision not to comply with the return or destruction obligation, (2) a receiving party's lack of technical acumen or ability, (3) a receiving party's difficulty in accounting for, or overlooking, trade secrets routinely backed up or archived and stored in memory the receiving party routinely uses to back up or archive its information, at least temporarily, (4) inability to remove notes or information

regarding trade secrets from internal notes or materials, or (5) human error. Such a failure may lead to a dispute between the parties and constitute, for example, trade secret misappropriation or a breach of contract, especially if the parties do not account for the failure in the NDA or another contract and the backed-up or archived trade secrets are not maintained in confidence.

The parties' NDA or other contract can address the possibility of the above failures by, for example, (1) obligating the receiving party to (a) confirm that the backed-up or archived trade secrets are destroyed, or permanently deleted, in the normal course of the receiving party's document retention or other applicable policy or (b) implement a specific technical solution, if feasible, and (2) specifying cure procedures and remedies for any breach of those obligations.

The parties can include a provision requiring the receiving party to explain, in writing, to the disclosing party any asserted justification for any non-return or non-destruction of a trade secret, including that return or destruction conflicts with a litigation hold, a trade secret is embedded in an attorney-client communication and part of a corresponding attorney-client privilege claim, or a trade secret is embedded in work product and part of a corresponding work product protection claim. Such an explanation may facilitate a solution, even if delayed, and may reduce the risk of a dispute that leads to litigation.[57] The parties can also include a provision authorizing the receiving party to securely archive copies of shared trade secrets. Such copies could be archived through, for example, a mutually approved third-party escrow service and be accessible to or used

57. As a practical matter, a receiving party with experience implementing and releasing a litigation hold may be able to apply that experience to comply with its return or destruction obligations.

by the receiving party, i.e., its counsel or specific receiving-party personnel, only in the event of a future dispute between the disclosing party and receiving party.[58] The above described process for the parties to confirm, in writing, what trade secrets have been shared can facilitate such archiving.

C. *Subsequent Work Relating to Trade Secrets Is Performed by the Receiving Party or by Receiving Party Personnel Who Depart and Work Elsewhere*

A potentially precarious situation exists where the receiving party engages in its own allegedly independent work relating to the trade secrets, the receiving party enters into a relationship with a third party where they engage in work relating to the trade secrets or receiving party personnel, such as employees, vendors, consultants and independent contractors, who acquired, accessed, reviewed, disclosed or used the trade secrets, take a new job or role where the new employer or partner is engaging in work relating to the trade secrets.

Four issues immediately can arise: (1) whether the receiving party returned or destroyed all the trade secrets, (2) whether the receiving party confirmed that it returned or destroyed all the trade secrets, (3) whether actual trade secret misappropriation, through unauthorized acquisition, disclosure or use, is taking place, and (4) whether trade secret misappropriation, through unauthorized acquisition, disclosure or use, is threatened, including whether such misappropriation is inevitable.[59]

---

58. The disclosing party's access to and use of the archived copies of shared trade secrets, i.e., its trade secrets, can justifiably not be so limited.

59. Inevitable misappropriation is a viable claim in some jurisdictions, but not in others, and is also a claim that can be asserted against an individual or entity. *See, e.g.*, PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995) *and* Certainteed Ceilings Corp. v. Aiken, Civil Action No. 14-3925, at *4 (E.D. Pa.

As discussed above, establishing and maintaining trade secret status for information requires that the information be the subject of reasonable protective measures. That obligation typically is tied to the circumstances. Thus, where the circumstances change as described above, the protective measures may need to be supplemented, modified or enhanced. A first step to reasonably supplementing, modifying or enhancing those protective measures may be to promptly notify the receiving party, in writing, of the circumstances and concerns and request confirmation, or re-confirmation, that the receiving party has returned or destroyed all the shared trade secrets and has complied and is complying with all other obligations, including non-use and non-disclosure obligations. A next step, which may be or include initiating litigation, will likely be driven by the receiving party's response or non-response.

As also discussed above, the parties may have accounted for some or all of the foregoing circumstances in a pre-litigation dispute provision in an NDA or another contract. The parties also may have specified, in one or more contracts, permissible and impermissible work or other activity, including new or

---

Jan. 29, 2015). *See also* Kinship Partners, Inc. v. Embark Veterinary, Inc., 3:21-cv-01631-HZ, at *13 (D. Or. Jan. 3, 2022) ('Several states recognize the inevitable disclosure [*sic*, misappropriation] doctrine under their respective trade secret misappropriation statutes.') (internal citation omitted); *and id.* ('Seventeen states appear to have adopted the inevitable disclosure [*sic*, misappropriation] doctrine in one form or another.') (internal citation omitted). California, Colorado, Louisiana, Maryland, Oregon, Virginia and the District of Columbia do not recognize—and, in some cases, have 'specifically rejected'—inevitable misappropriation as a form of threatened misappropriation and, as such, as a basis for relief. *Certainteed*, at *4; *and Kinship,* at *13 n.3. As to federal law, the consensus is the DTSA, which expressly provides relief for any actual or threatened misappropriation, does not encompass or provide relief for inevitable misappropriation by an individual. *See* 18 U.S.C. § 1836(b)(3)(A)(i)(I), (II).''), *and id.* at 12–13.

expanded business relationships, after due diligence or the relationship ends, with such provisions addressing, for example, covered subject matter, walling off receiving-party personnel and the duration of any restrictions.

D. Receiving Party or Receiving Party Personnel Are Pursuing, Later Pursue or Enter Relationship with a Competitor of Disclosing Party

Two of the precarious situations addressed above can become riskier where a third-party competitor of the disclosing party is involved. That is, where (1) the receiving party is pursuing, later pursues, or enters into a relationship with a competitor of the disclosing party and they engage in work relating to the trade secrets, or (2) receiving party personnel such as employees, contractors, vendors, consultants and independent contractors who acquired, accessed, reviewed, disclosed or used the trade secrets, take a new job or role where the new employer or partner is a competitor of the disclosing party and engaging in work relating to the trade secrets, the risk of unauthorized acquisition, disclosure or use of the trade secrets can increase. These situations may become more complicated if the competitor of the disclosing party denies that the claimed trade secrets are entitled to trade secret protection. An NDA or other contract can address these circumstances, bearing in mind that contractual restrictions or prohibitions on an entity's activity or relationships can be distinct from and more easily enforced than contractual restrictions or prohibitions on an individual's activity or relationships, such as new employment or other roles.

E. Receiving Party Hires or Retains Disclosing Party's Present or Former Personnel

Another potentially precarious situation is where disclosing party personnel, such as a present or former employee, are hired

by the receiving party after due diligence or a relationship between the disclosing party and receiving party ends. Such hiring poses a risk that the former disclosing party employee will perform work for the receiving party that involves trade secret misappropriation, i.e., actual or threatened, including inevitable, disclosure or use of one or more of the disclosing party's trade secrets. Importantly, the trade secrets at issue may include trade secrets the disclosing party shared with the receiving party and trade secrets the disclosing party did not share with the receiving party. A first step for the disclosing party may be to notify the receiving party, in writing, of the circumstances and concerns and request confirmation, or re-confirmation, that the receiving party has complied and is complying with all applicable obligations and, to the receiving party's knowledge, the former employee has and is as well. A next step, which may be or include initiating litigation, will likely be driven by the receiving party's response or non-response.

The parties may have accounted for the foregoing circumstances in a pre-litigation dispute provision in an NDA or another contract. The parties also may have specified, in an NDA or another contract, permissible and impermissible solicitation, recruitment, interviewing and hiring practices involving current and former personnel, including employees. Whether non-solicit, non-recruit or noncompete provisions or other employment-related restrictions are enforceable largely depends on the jurisdiction. Recent developments relating to noncompetes, including the increasing number of states banning or limiting noncompetes and agreements that have a similar effect, necessitate that confidentiality, including non-disclosure, obligations are properly focused on protecting the trade secrets and other protectible interests at issue.

A receiving party can mitigate the risks described above by designing and implementing an onboarding, including

interviewing, process that includes, for example: (1) obtaining and reviewing a copy of any non-confidential restrictive covenant into which the new employee has previously entered and, as permitted, obtaining and reviewing a copy of any confidential restrictive covenant into which the new employee has previously entered; (2) obtaining from the new employee a signed, written verification that (a) the new employee is not violating and will not violate an obligation to a former employer by accepting and undertaking the new employment, (b) the new employee has fully complied with all return and destruction obligations (e.g., regarding any device, trade secret or other information) of the former employer, and (c) the new employee does not possess, on any device or in any tangible (e.g., paper or electronic) form, any trade secret or other confidential, secret or proprietary information of the former employer; (3) establishing, in writing, the new employee's obligations to the new employer, including not to acquire, access, disclose or use any trade secrets, or other confidential, secret or proprietary information, of the former employer; (4) ensuring the new employee is educated on confidentiality, including the new employer's corresponding policies and procedures; (5) obtaining an executed confidentiality agreement between the new employer and new employee; (6) maintaining a completed, signed onboarding checklist in the new employee's file; and (7) ensuring the new employee is not performing and does not perform work that involves, or unreasonably risks involving actual or threatened, including inevitable, disclosure or use of the former employer's trade secrets.[60] All the above steps might not be possible, or might not be performed in a particular company setting.

60. The above discussion expressly addresses employees and employers. It also can apply to other relationships involving other personnel, such as vendors, consultants and independent contractors.

Relatedly, differences in applicable law can inform or modify aspects of an onboarding process. But where a receiving party hires a disclosing party's personnel, such as a present or former employee, the receiving party can balance its resources with the opportunity and need to protect itself.[61]

F. Considerations when Sharing Trade Secrets Internationally

International sharing of trade secrets raises unique issues when due diligence or a relationship ends.[62] As an initial matter, proper identification of trade secrets is particularly important where trade secrets are shared internationally, as enforcement can be especially difficult without proper identification. Further, given the rise of economic espionage in an increasingly globalized, digital business world with more frequent cross-border sharing of trade secrets, disclosing parties often need a systematic approach to protect their trade secrets and promptly enforce them. Of course, the approach will differ depending on the disclosing party, its resources, the receiving party and the country or countries at issue.

Despite those unique issues, where a disclosing party intends to share trade secrets with a foreign receiving party, the disclosing party can proceed by accounting for the same or similar issues it accounts for when sharing trade secrets with a domestic receiving party. The disclosing party's focus would be protecting its trade secrets, anticipating and preparing for

---

61. The Sedona Conference, *Commentary on Protecting Trade Secrets Throughout the Employment Life Cycle*, 23 SEDONA CONF. J. 807 (2022), substantively analyzes, for example, trade secret considerations that can arise in connection with employees.

62. For in-depth analysis regarding issues related to international sharing of trade secrets, *see* The Sedona Conference, *Framework for Analysis on Trade Secret Issues Across International Borders*, 23 SEDONA CONF. J. 909 (2022).

litigation to enforce its rights and considering the following:

a. Discovery is less available for litigation in international forums,[63] so consider being vigilant in tracking, documenting, and managing any documents and activity relating to sharing trade secrets in case a dispute arises.

b. Take steps set forth in Section IV(B) to the extent available and applicable to trade secrets disclosed to a foreign receiving party.

c. Pursuant to a contract with the receiving party, consider memorializing the identification and a list of the shared trade secrets at an appropriate time, to an appropriate degree, and in an appropriate manner.

d. Consider documenting the return and destruction of trade secrets by the receiving party.

e. Pursuant to a contract with the receiving party, consider memorializing ownership, retention,

63. For additional guidance, *see* The Sedona Conference, *Commentary on Cross-Border Discovery in U.S. Patent and Trade Secret Cases ("Stage Two")*, 24 SEDONA CONF. J. 549 (2023).

and other rights and interests in and to any modified or jointly developed trade secrets.

f. Ensure compliance with applicable data protection or transfer laws.

g. To the extent the disclosing party discovers or believes that trade secrets were or are being misappropriated during due diligence or the relationship, but the disclosing party still wants or needs services of the receiving party because of, for example, business reasons, consider a strategy to document and effectuate the disassociation of the parties. The strategy would seek to limit and, if possible, eliminate through contractual, physical and technological tools, the receiving party's current and future acquisition, access, review, disclosure, and use of the trade secrets, while ensuring sufficient time and opportunity to comply with applicable statutes of limitation for a trade secret misappropriation or other action.[64]

h. Consider choice of law and potential forums and venues for any dispute. As discussed in Section IV.C.1 above, parties can include choice of law and forum and venue selection provisions in an NDA or another contract. International trade secret sharing can elevate the importance of those

64. Ping-Hsun Chen, Trade Secret Protection Against Misappropriation Committed by Your Foreign Distributor-A Lesson from Atricure, Inc. v. Jian Meng, 102 JOURNAL OF THE PATENT AND TRADEMARK OFFICE SOCIETY, 252, 263 (2022).

provisions. The different potential forums for disputes have various costs and benefits for the disclosing party and receiving party.[65]

i. Regarding points a and h above, U.S. Courts increasingly offer a relatively favorable environment for companies to pursue trade secret misappropriation claims against foreign defendants. U.S. Courts interpreting both the DTSA and some States' versions of the UTSA are permitting extraterritorial misappropriation claims.[66] But given the difficulty in obtaining

---

65. For in depth-analysis of issues relating to the forums and legal regimes chosen for disputes over internationally shared trade secrets, including various U.S. State Courts, U.S. District Courts, the U.S. International Trade Commission, the Economic Espionage Act of 1996, regulatory actions and the World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property Rights, *see* The Sedona Conference, *Framework for Analysis on Trade Secret Issues Across International Borders*, 23 SEDONA CONF. J. 909 (2022).

66. *See, e.g.*, DTSA, 18 U.S.C. § 1837; vPersonalize Inc. v. Magnetize Consultants Ltd., 437 F. Supp. 3d 860, 878–79 (W.D. Wash. 2020) (stating that "18 U.S.C. § 1837 authorizes civil enforcement actions against foreign entities to the same extent as criminal actions" and collecting cases); Motorola Sols., Inc. v. Hytera Commc'ns Corp., 436 F. Supp. 3d 1150, 1165 (N.D. Ill. 2020) ("the Court holds that the DTSA may apply extraterritorially in this case because the [act in furtherance] requirement of [18 U.S.C. § 1837(2)] has been met"), Motorola Sols., Inc. v. Hytera Commc'ns Corp., 108 F.4th 458, 488 (7th Cir. 2024) (*rev'd in part, aff'd in pertinent part and remanded*) *and* Motorola Sols., Inc. v. Hytera Commc'ns Corp., 2024 WL 4416886 (7th Cir. 2024) (petition for rehearing *en banc* denied); AtriCure, Inc. v. Jian Meng, 842 F. App'x 974, 983 (6th Cir. 2021) (holding the Ohio UTSA applies extraterritorially against Chinese defendants concerning conduct in China); *and* Miller UK Ltd. v. Caterpillar Inc., No. 10-CV-03770, 2017 WL 1196963, at *7 (N.D. Ill. Mar. 31, 2017) (concluding the Illinois Trade Secrets Act, 765 ILCS 1065/1 *et seq.* (ITSA) has extraterritorial effect because the ITSA specifically states that "a contractual or other duty to maintain secrecy or limit use of a trade secret shall not be

foreign discovery, especially in a U.S. district court or State court action, potential personal jurisdiction issues and enforcing any remedy, disclosing parties, i.e., potential plaintiffs, need to be well organized in collecting evidence for such claims prior to, during, and after exiting due diligence or a relationship involving sharing trade secrets with a foreign receiving party.

j. Regarding points a and h above, the U.S. International Trade Commission likewise offers a relatively favorable environment for companies to pursue trade secret misappropriation claims against foreign respondents.

---

deemed to be void or unenforceable solely for lack of durational or geographical limitation on the duty.").

VII. APPENDIX

Parties can consider the following points before and when sharing trade secrets.

Disclosing Party

- What is the fewest number of trade secrets that can be shared to satisfy the purpose?
- Can the disclosure consist of physical documents or electronic files that can be marked and traced?
- What is the fewest number of individuals who need access to, i.e., need to know, the shared trade secrets?
- Can any such access be limited in time, by device or access point, by purpose or otherwise?
- What are the tools the disclosing party uses to protect its trade secrets?
- What are the tools, including supplemental, modified, or enhanced tools, the receiving party needs to use to protect the trade secrets?
- Is an NDA or other agreement in place? If so, are the following provisions in effect or needed:
    - Identification of trade secrets
    - Marking requirement, including in connection with oral disclosures
    - Authorized and unauthorized individuals (or titles)
    - Modification of, derivation from and joint development of trade secrets and other assets
    - Legal and regulatory obligations, including disclosures and corresponding cooperation

  - Ending of due diligence or relationship, including return or destruction obligations
  - Milestone events in NDA or other agreement, including results or consequences
  - Audit, inspection and examination rights
  - Reverse engineering prohibition
- Is another contractual tool, such as a noncompete, in place or a necessary and available option?
- What are the technological tools to be used by the receiving party to protect the trade secrets?
- What are the physical tools to be used by the receiving party to protect the trade secrets?
- Will there be international sharing of the trade secrets? If so, are there corresponding laws or regulations to be considered?
- Are there applicable third-party obligations or issues?

Receiving party

- What is the fewest number of trade secrets that can be shared to satisfy the purpose?
- Can the disclosure consist of physical documents or electronic files that can be marked and traced?
- What is the fewest number of individuals who need access to, i.e., need to know, the shared trade secrets?
- Can any such access be limited in time, by device or access point, by purpose or otherwise?
- What are the tools the disclosing party uses to protect its trade secrets?

- What are the tools, including supplemental, modified or enhanced tools, the receiving party needs to use to protect the trade secrets?
- Is an NDA or other agreement in place? If so, are the following provisions in effect or needed:
    - Identification of trade secrets
    - Marking requirement, including in connection with oral disclosures
    - Authorized and unauthorized individuals (or titles)
    - Modification of, derivation from and joint development of trade secrets and other assets
    - Residuals clause
    - Feedback clause
    - License
    - Legal and regulatory obligations, including disclosures and corresponding cooperation
    - Ending of due diligence or relationship, including return or destruction obligations
    - Milestone events in NDA or other agreement, including results or consequences
- What are the technological tools to be used by the receiving party to protect the trade secrets?
- What are the physical tools to be used by the receiving party to protect the trade secrets?
- Is a non-exclusive right to evaluate or work in the area pertaining to the trade secrets needed?
- In a supply relationship, is an obligation to continue supplying for a period under reasonable terms needed?

- Will there be international sharing of the trade secrets? If so, are there corresponding laws or regulations to be considered?
- Are there applicable third-party obligations or issues?

A Project of The Sedona Conference Working Group (WG12) on Trade Secrets

Author

The Sedona Conference

Editors-in-Chief

David Almeling Vicki Cundiff

Managing Editor

Casey Mangan

Senior Editor

Lauren Linderman

Contributing Editors

Jeremy Elman John Gray
Angelique Kaounis Kate Lazarus
Teresa Lewi Nate McPherson
Lisa Zang

Staff Editor: Craig Morgan

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 12. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

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

This publication may be cited as follows:

> The Sedona Conference, *Commentary on the Use of Clean Rooms*, 26 SEDONA CONF. J. 299 (2025).

PREFACE

Welcome to the August 2025 Final Version of The Sedona Conference's *Commentary on the Use of Clean Rooms*, 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, artificial intelligence, and data security and privacy law. The Sedona Conference mission 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 Clean Rooms Brainstorming Group was launched in January 2023. Earlier drafts of this publication (including the Brainstorming Group project charter) were a focus of dialogue at the WG12 Annual Meeting in Minneapolis, Minnesota, in September 2023, and the WG12 Annual Meeting in Phoenix, Arizona, in September 2024. 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, the Chair of WG12, and

Victoria Cundiff, now Chair Emeritus of WG12, who serve as the Editors-in-Chief of this *Commentary*, and Lauren Linderman who serves as the Senior Editor 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 Jeremy Elman, John Gray, Angelique Kaounis, Kate Lazarus, Teresa Lewi, Nate McPherson and Lisa Zang.

The drafting process for this *Commentary* has also been supported by the Working Group 12 Steering Committee and WG12's Judicial Advisor for this *Commentary*, the Hon. Hildy Bowbeer (ret.). 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 artificial intelligence and the law, electronic document management and discovery, cross-border discovery and data protection law, international data transfers, data security and privacy liability, 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. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Kenneth J. Withers
Executive Director
The Sedona Conference
August 2025

TABLE OF CONTENTS

THE USE OF CLEAN ROOMS PRINCIPLES & GUIDELINES "AT A GLANCE"

PRINCIPLE 1: A Clean Room is an approach to reduce the risk of trade secret misappropriation, document independent development efforts, and/or protect innovation where the development process might otherwise be—or be alleged to have been—exposed to or influenced by Outside Protected Information.

GUIDELINE 1: A Clean Room Protocol describes the purpose and operation of the Clean Room. This documentation can take many forms.

GUIDELINE 2: The Clean Room participants should be aware that the purpose of the Clean Room is to confirm and document independent development; whether to provide further context depends on the specific situation.

PRINCIPLE 2: The Clean Room should take reasonable measures to avoid the use of Outside Protected Information.

GUIDELINE 1: The information that qualifies as Outside Protected Information should be identified.

PRINCIPLE 3: The Manager(s) of the Clean Room process must be sufficiently familiar with the underlying issues to be able to identify people to be involved or excluded.

PRINCIPLE 4: Counsel may be uniquely positioned to consult on the design of the Clean Room and whether the processes for the Clean Room are appropriate in view of the legal landscape, litigation concerns, or other legal concerns the company may have.

GUIDELINE 1: It is often, but not always, necessary for counsel to participate in the Clean Room process. Counsel, both inside and outside, will often play a crucial role in developing and implementing a Clean Room process and may be involved in one or more of the following functions.

PRINCIPLE 5: When legal counsel is involved in a Clean Room development process, care should be taken to avoid inadvertent and unintended waiver of privilege or work product protections connected to the involvement of counsel or, if waiver is reasonably foreseeable, measures should be taken to plan and define the scope of the intentional waiver.

GUIDELINE 1: To avoid inadvertent waiver or intentional waiver with an unintended scope, consider whether the role of counsel and what aspects of Clean Room development counsel is working on should be clearly defined and memorialized.

GUIDELINE 2: To avoid inadvertent waiver or intentional waiver with an unintended scope, consider whether to divide responsibilities among separate legal counsel, such as by having one counsel advise on issues where waiver is foreseeable and a separate counsel advise on issues where waiver is not foreseeable.

PRINCIPLE 6: A Clean Room Protocol should clearly describe the restrictions put in place to prevent the Clean Team from using or incorporating Outside Protected Information in product development.

GUIDELINE 1: To enable participants and evaluators of a Clean Room to understand the purpose of the Clean Room development, it may be helpful for the Protocol

to set forth a description of the purpose of the Clean Room.

GUIDELINE 2: To allow relevant individuals to identify the Outside Protected Information that should not be used by the Clean Team, consider whether the Protocol should describe, without disclosing, the Outside Protected Information.

GUIDELINE 3: To maintain an accurate record of Clean Room participants and facilitate compliance with the Clean Room Protocol, consider whether the Protocol should identify the individuals on the Clean Team, any individuals with exposure to or familiarity with the Outside Protected Information (such as those on the Dirty Team), the Manager(s), and/or any Monitor of the Clean Room.

GUIDELINE 4: To ensure that Clean Room participants understand their obligations and the procedures to be followed under the Protocol, consider whether the Protocol should contain clear instructions and procedures for the Clean Room and whether the Company should maintain records of such instructions and procedures.

GUIDELINE 5: To document that Clean Room participants and other relevant individuals will comply with the Protocol, consider whether the Protocol should include a signed acknowledgement.

I. INTRODUCTION

A "Clean Room" is a development process designed to limit or minimize the risk of legal liability and allegations of unlawful conduct that might otherwise result if the development process were exposed to or influenced by certain information from outside the company to which the company does not have rights. Utilizing a Clean Room development process can be an effective way to develop new proprietary material (whether software, mechanisms, algorithms, business methods, or any other intellectual property) while minimizing concerns about the material's origin. The Clean Room method utilizes an isolated development environment where the possibility that certain information influences the development process is eliminated or significantly mitigated. The Clean Room is intentionally kept free from certain information and influence of third parties, such as confidential or trade secret information, copyrighted materials, licensed materials, or other nonpublic or protected information.

By conducting a development process in a Clean Room, companies take steps to ensure their creations are not the result of copying preexisting works, and that similarities, if any, between the created material and any preexisting material are coincidental. Use of a Clean Room can be an effective tool to avoid or defend against claims for, among other things, breach of a confidentiality agreement or trade secret misappropriation. A Clean Room may also be used as a tool to support (or refute) a defendant's independent development or reverse engineering claim in trade secret litigation by demonstrating that the product or information was independently developed or, alternatively, that it could not have been the result of independent development.

Designing and implementing a Clean Room may, in some situations, be a time-consuming and expensive endeavor, but it can also be critical to minimizing risk and protecting innovations. Whether to implement and how to design the Clean Room should be carefully evaluated by an organization. It is recommended that companies consult with counsel to determine whether, when, and how to implement a Clean Room, and to assist in the design and implementation of the Clean Room.

A Clean Room's effectiveness depends on its proper implementation and on relevant parties following its requirements. But there is no one-size-fits-all approach for creating and implementing a Clean Room. As such, this *Commentary* makes recommendations regarding Clean Room design that are not intended to be mandatory in any or every situation; the failure to follow the recommendations set forth in this *Commentary* does not necessarily mean the Clean Room was ineffective, just as following every recommendation set forth in this *Commentary* does not necessarily mean the Clean Room was effective. Nor should an organization's following or failure to follow the recommendations set forth in this *Commentary* be dispositive on issues relating to, for example, reasonable efforts to maintain the secrecy of trade secrets. Instead, the goals of the *Commentary* include: (1) providing a foundation for practitioners to understand what a Clean Room is, why one would be used, and when to consider using one; and (2) identifying features that may be incorporated into a Clean Room process, including identifying the key players that may be involved in designing and implementing a Clean Room. To help achieve these goals, we include as Appendix A, a Sample Clean Room Protocol.

This *Commentary* does not address whether a particular form of Clean Room procedure is certain to withstand scrutiny if challenged in any subsequent litigation because the Clean Room procedures discussed in this *Commentary* are not intended to be

used solely for litigation purposes, and because such a conclusion depends on the circumstances at issue and is a question of fact to be determined by a judge, jury, or other fact finder.[1]

II. WHAT IS A CLEAN ROOM AND WHEN SHOULD A CLEAN ROOM BE CONSIDERED?

A. Definition of a Clean Room

A "Clean Room" is a development process designed to limit or minimize the risk of legal liability and allegations of unlawful conduct that might otherwise result if the development process were exposed to or influenced by certain information—e.g., confidential or trade secret material from outside the company to which the company does not have—or may be argued not to have—rights (hereinafter "Outside Protected Information").[2] As such, a Clean Room is a deliberate form of an independent development project, often with specific protocols or procedures, designed to restrict or prevent improper or unauthorized reference to or reliance upon Outside Protected Information during development. A Clean Room development process may include, for example, isolating and/or vetting engineers, designers, or developers (the "Development Team") to limit or prevent

1. Other related Sedona Conference commentaries provide useful guidance regarding Clean Rooms and related topics, including: The Sedona Conference, *Commentary on the Governance and Management of Trade Secrets*, 24 Sedona Conf. J. 429 (2023), available at https://thesedonaconference.org/publication/Commentary_on_Governance_and_Management_of_Trade_Secrets (discussing trade secret protection programs, including clean rooms).

2. A Clean Room may also be used in other contexts and for other purposes, including civil and criminal claims at both the state and federal levels. The Sedona Conference Working Group 12 on Trade Secrets, and this *Commentary*, focuses on Clean Rooms in the context of trade secrets liability.

their access to or use of Outside Protected Information such that the possibility of Outside Protected Information influencing the development process is eliminated or significantly mitigated.

The specific protocols or procedures of a Clean Room development process may differ based on the circumstances, the type of technology, the type of information involved, the capabilities or resources of the parties, the business or litigation reasons for creating the Clean Room, the history of those involved, prior development efforts, the status of general knowledge and skill in the relevant art, the level of acceptable risks given the stakes at hand, and other factors.

As discussed in further detail below, components of Clean Rooms may include: a development team that is screened from and does not have knowledge of Outside Protected Information; a team that defines the specification used by the development team; a monitor, facilitator, or other means to ensure that Outside Protected Information is screened from the development team; and a written instruction protocol for implementing a Clean Room.

The Clean Room development process may also encompass situations where there may be a need for an employee who has had access to Outside Protected Information to be involved in some aspect of the Clean Room development process. In these situations, a company may consider employing additional or alternative safeguards to further mitigate the possibility of Outside Protected Information influencing the development process.

B. Scenarios in which a Clean Room Should be Considered

There are several different scenarios in which a company may utilize a Clean Room, as further discussed in Part III.A, below. Some examples include the following:

- When a company has had access to Outside Protected Information—e.g., by virtue of a license agreement, a possible licensing relationship that does not come to fruition, a non-disclosure agreement ("NDA"), a failed collaboration, merger, or joint venture, etc.—and intends to develop a similar or competing product;
- When hiring another company's former employee who had access to that company's Outside Protected Information that might provide, or be perceived to provide, a benefit to the new employer;
- In response to allegations of misconduct or during litigation, to support an independent development or reverse engineering defense to a trade secret misappropriation claim;
- After litigation, as part of a settlement or court-ordered remedy; or
- Other situations where a company or its employees might have had access to Outside Protected Information and the company wishes to take precautions to limit liability and allegations of unlawful conduct based on improper use of that Outside Protected Information in development.

III. HOW TO DESIGN A CLEAN ROOM AND WHO SHOULD BE INVOLVED IN THE PROCESS?

A. Identifying the Purpose of the Clean Room

Principle 1: A Clean Room is an approach to reduce the risk of trade secret misappropriation, document independent development efforts, and/or protect innovation where the

development process might otherwise be—or be alleged to have been—exposed to or influenced by Outside Protected Information.

Guideline 1: A Clean Room Protocol describes the purpose and operation of the Clean Room. This documentation can take many forms.

Guideline 2: The Clean Room participants should be aware that the purpose of the Clean Room is to confirm and document independent development; whether to provide further context depends on the specific situation.

Clean Rooms serve different purposes, and how a party implements a Clean Room may depend on the particular purpose. Companies may consider Clean Rooms in several common scenarios.

Litigation-related scenarios

A company may set up a Clean Room when it is in litigation or suspects that litigation is reasonably likely. In this case, one of the primary purposes of the Clean Room is to develop evidence the company could use in litigation. Sometimes, an expert witness could be involved in establishing the Clean Room, and other times the company may do the work alone. Either way, in this scenario, clearly documenting procedures and each step of the Clean Room can help build the record the company may want to use during litigation. (This is not to say that a formal Clean Room is necessary to prove that a company developed a product independently, or that use of a Clean Room will establish independent development.)

Clean Room development can also be part of a litigation settlement or ordered as part of an equitable remedy by a court.

For example, a party to a litigation may agree or be ordered to rewrite specific sections of software code in a Clean Room environment where the code has already been determined to contain, to have used in development, or otherwise to misappropriate Outside Protected Information. See, e.g., Oakwood Labs. LLC v. Thanoo, 999 F.3d 892, 910 (3d Cir. 2021) ("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 'assist[ing] or accelerat[ing] research or development.").

Non-litigation related scenarios

A company might voluntarily use a Clean Room even where it faces no salient risk of litigation because it wants to reduce the chances that its products contain Outside Protected Information that the company possesses. For example, a company might receive Outside Protected Information under an NDA as part of joint development work, joint ventures, customer/vendor relationships, merger and acquisition discussions, or any number of business dealings. Sometimes, that information could relate to a product the company wants to develop. Even if the company disclosing the Outside Protected Information has not threatened a claim for trade secret misappropriation or other misuse of the Outside Protected Information, the receiving company might institute a formal Clean Room as a precautionary measure. As another example, a Clean Room may be used to produce a device that can interoperate with another device that contains the Outside Protected Information. In yet another example, a company may want to use a Clean Room to reverse engineer and copy the functionality of some other party's product without using Outside Protected Information incorporated into that product known to the company or incoming employees at the company.

Clean Room development can also be implemented between parties that wish to share and protect limited Outside Protected Information, such as for a joint venture or other joint product development. In this case, one party may give limited Outside Protected Information to the joint developers but withhold other Outside Protected Information from developers in the Clean Room that does not directly relate to the product being jointly developed. This helps ensure that the Clean Room development team has only limited information, which can help protect both participants in the joint development from the misuse (or even the perceived misuse) of Outside Protected Information that should not be used as part of the joint product development. In this way, a Clean Room can be an important and useful development tool in situations where companies share Outside Protected Information pursuant to a written contract that explicitly states which information can be shared and which information cannot be shared or that otherwise places restrictions on the use of Outside Protected Information. For example, Company A and Company B might have technical information about how each of their product components work, and they share that information to help a joint development team combine those components into a single usable product. But Company A and Company B may also have other technical information about other components or about other aspects of product development; that information may be excluded from the Clean Room to ensure that the Clean Room team does not have exposure to the information.

The procedures employed for any given Clean Room project may vary depending on the circumstances and can be described as falling on a spectrum: Some Clean Rooms may have extremely rigorous and well-documented (and more expensive) procedures, others may have less-rigorous procedures that are still sufficient to protect against the unauthorized use of Outside

Protected Information, and others may fall anywhere in between. Whether any particular restriction or set of restrictions is appropriate will depend on the situation, including the information, companies, industries, and product development involved, among other things. Therefore, the protocol and procedures described in this Commentary may not be necessary or even appropriate for every product development scenario. While a company may want (or in some cases, need) to use a Clean Room, in general, trade secret law does not mandate the use of Clean Rooms for a company to show that it has not misappropriated trade secrets,[3] and use of or failure to utilize any of the restrictions described herein is not dispositive of whether an independent development effort was truly "independent" of Outside Protected Information.

B. Identifying what is Outside Protected Information

Principle 2: The Clean Room should take reasonable measures to avoid the use of Outside Protected Information.

Guideline 1: The information that qualifies as Outside Protected Information should be identified.

The particular information that qualifies as Outside Protected Information will vary. Companies should consider at least the following issues.

---

3. *See, e.g.*, Adacel, Inc. v. Adsync Tech., Inc., 2020 WL 4588415, at *3 (M.D. Fla. July 9, 2020) (allowing the plaintiffs' expert to rebut the defendant's expert opinion describing how the defendant could have proceeded without misappropriating the plaintiffs' information "in so far as Defendant failed to use *one accepted method* [a clean room] for ensuring that no trade secrets were used" (emphasis added)).

(1) If the information is subject to an NDA or other contractual confidentiality obligation, carefully review the agreement to assess whether information falls under the NDA. In some cases, not all information that the disclosing company provides to the receiving company will qualify as Outside Protected Information under an NDA. In other cases, documents or information beyond what the disclosing company provided may constitute Outside Protected Information.

(2) Although less common, a company might also possess Outside Protected Information even if that information is not governed by an NDA. In that situation, the Clean Room company should consider whether the information qualifies as a trade secret under the applicable law, as well as whether the information is protectable as non-trade secret proprietary or confidential information.

After the company and/or its counsel, as discussed below, decides what qualifies as Outside Protected Information for purposes of the Clean Room, steps should be taken to ensure that the Clean Room participants understand what is and is not Outside Protected Information, such as by defining that information in a Clean Room Protocol, which can help ensure there is a clear record of what is and is not allowed in the Clean Room.

Depending on the situation, a company may want to exclude more information from the Clean Room than is required under contract or other law. That could be to reduce the company's risk, for business-relationship reasons, or practicality reasons. If that is the case, the company should consider whether to document that it is being over-inclusive so that it does not inadvertently create a record suggesting that more information is protectable than really is.

C. Identifying the people

Principle 3: The Manager(s) of the Clean Room process must be sufficiently familiar with the underlying issues to be able to identify people to be involved or excluded.

As a step in setting up a Clean Room, it is recommended that efforts be made to determine the relevant people who may have some involvement in the Clean Room process. Depending on the circumstances, this can include identifying:

- Who will manage the set-up of the Clean Room ("Manager(s)")?
- Which employees will be involved with the development of the product in the Clean Room?
- Which employees will be involved with the development of any specification the development team will use?
- Which employees, if any, have had exposure to the Outside Protected Information?
- Who, if anyone, will serve as the monitor for the Clean Room development ("Monitor(s)")?
- What will be the role, if any, of inside or outside counsel in the Clean Room process?

1. Individuals who will be involved with the Clean Room development process

Someone or a small group of people—the "Manager(s)"—should be involved in setting up the Clean Room (and the other activities, described below). This often will be legal counsel, but it need not be. The Manager(s) can manage and supervise the entire Clean Room set-up process, such as identifying the individuals who should be involved in the Clean Room

development and who should be excluded, developing a Clean Room Protocol, supervising its implementation and progress, and addressing any questions as they may arise. The Manager(s) may or may not also be the Monitor (discussed below).

Although circumstances will differ, the Manager(s) should exercise such control and supervision as is reasonably necessary under the circumstances to make compliance with the Clean Room Protocol reasonably likely. This may include conducting periodic check-ins to, for example, assess the continued need for the Clean Room, confirm no one on the Clean Team has had unauthorized access to Outside Protected Information, and ensure the correct people are involved in the Clean Room development, among other things. The Manager(s) do(es) not necessarily need to be involved with every decision relating to the Clean Room, as many decisions may be handled by the individual employees participating in the Clean Room. However, the Manager's control and oversight should be consistent with the understanding that s/he may be held accountable for the effectiveness of the Clean Room development process.

The Clean Room should usually (though not always, see below) include individuals who are screened from and/or confirmed not to have knowledge of or exposure to Outside Protected Information—the "Clean Team." These are typically product development employees who did not have exposure to the Outside Protected Information, and in some cases depending on the circumstances and the resources available to the company, it may make sense to hire a brand-new team.

2. Individuals who may have had exposure to Outside Protected Information

In some situations, there may be individuals at the company who have had or may have had exposure to Outside Protected

Information, whether by virtue of prior employment, authorized disclosure as part of the ordinary course of their job duties, or some other reason. It is often advisable to identify such individuals at the outset of the Clean Room development project. In most cases, individuals who have had exposure to Outside Protected Information will be screened from being on the Clean Team or otherwise participating in the development taking place in the Clean Room; out of an abundance of caution, individuals who may have had exposure to Outside Protected Information may also be screened out. In short, and to the extent practicable under the circumstances, anyone who may reasonably be thought to have had exposure to or familiarity with the Outside Protected Information ordinarily should not be on the development team.

In certain situations, however, it may not be possible or practical for a company to completely screen individuals who were exposed to Outside Protected Information from a Clean Room development project, e.g., when a certain employee has a unique skill set required for a development project or is a key decision-maker whose input and/or involvement in a development project is necessary. In these situations, additional safeguards may be employed to eliminate or at least significantly mitigate the possibility of Outside Protected Information influencing a Clean Room development process.

a. Screening employees who may have had exposure to Outside Protected Information from a Clean Room development project

As previewed above, if a company employee had access to Outside Protected Information, that employee will frequently be screened from a Clean Room development process. In such situations, that employee may be instructed not to communicate with the Clean Team or, at least, not to convey any Outside

Protected Information to any member of the Clean Team. The Clean Team may similarly be instructed not to communicate with that employee about the Clean Room development process.

If a Clean Room development process is subject to subsequent evaluation (such as by a court or other outside party), the evaluator may closely scrutinize whether and to what extent there were communications between the Clean Team and any individuals who may have had access to Outside Protected Information, along with the content of any such communications. Where this scrutiny is likely or foreseeable, it may be advisable to block or limit direct communication between these two groups. This may not be practical in every situation, however, as the two groups may need to communicate, for example, on unrelated subject matter or on subject matter related to the product being developed that does not implicate Outside Protected Information.

Ultimately, if employees who had or may have had access to Outside Protected Information are screened from a Clean Room development project, the design of the Clean Room should give careful attention to whether there can be any direct communications between those employees and members of the Clean Team and, if so, what procedures or protections should be put in place relating to those communications. Such procedures or protections could include instructions to keep such communications minimized, a prohibition on direct communications relating to the Clean Room development, and/or the use of a monitor to screen or be copied on all such communications, as discussed in the next section. A company may also consider having the employees with access to Outside Protected Information sign assurances saying that they have not provided Outside Protected Information to the Clean Team.

b. Use of a "Dirty Room" / "Dirty Team" and other safeguards for situations when individuals who previously had access to Outside Protected Information have some role in a Clean Room development project

As already discussed, in view of business realities, technical and geographic limitations, or for other reasons, persons who had access to Outside Protected Information may be necessary to a development project. For example, an executive who was previously involved in due diligence may need to be involved in a subsequent development project to supervise the overall development and approve the final product. As another example, an employee with a certain unique skill set may need to be involved in both the evaluation of third-party technology and the subsequent development of a company's own home-grown technology. In these situations, a company may still use various components of a Clean Room process but may wish to employ additional or alternative safeguards and processes to eliminate or at least mitigate the possibility of Outside Protected Information influencing the development process.

As one example, a Clean Room development project may include a team of individuals separate from the Clean Team who have access to information about an existing product that is available to them, regardless of whether that information constitutes Outside Protected Information—referred to as a "Dirty Team" operating in a "Dirty Room." The Dirty Room can contain documents, data, and other information, including Outside Protected Information (assuming the inclusion of such information is not barred by any applicable agreements or law) to understand the product's functionality and how to interface with it. The Dirty Team may then be tasked with preparing a functional specification to be given to the Clean Team that

describes the required features of the product that will be developed in the Clean Room, but that does not include or reference any Outside Protected Information and that is not derived from and does not otherwise make use of Outside Protected Information.

In situations where a Dirty Room or Dirty Team is utilized, the purpose of the Dirty Room, how the Dirty Room and/or Dirty Team interacts with the Clean Room, the Clean Team or the Monitor (if used) should be specified in the Clean Room Protocol. That Protocol may also describe what additional safeguards a company may employ to ensure that Outside Protected Information does not inadvertently get transferred from the Dirty Room to the Clean Room, such as, for example, requiring that all communications and documentation sent by the Dirty Room to the Clean Room first be reviewed by the Monitor, or requiring that any specification prepared in the Dirty Room must directly link any product requirement to public information or the Company's previously documented know-how. A separate Dirty Room Protocol may also be prepared.

In addition, a company may employ other safeguards to eliminate or at least mitigate the risk that Outside Protected Information will influence a Clean Room development project, where an employee who was exposed to Outside Protected Information is a necessary participant in the development project. Such additional safeguards include, for example:

- Limiting that employee's involvement to an area unrelated to Outside Protected Information or where that employee's expertise is necessary for the development project.
- Conducting an audit of the work performed by, or contributions of, that employee to confirm no Outside Protected Information was used.

- Limiting the involvement of that employee to providing high-level guidance, e.g. regarding desired product attributes, or to approving or rejecting the end product of the development project.
- Requiring that employees who had access to Outside Protected Information sign assurances saying that they have not provided Outside Protected Information to the Clean Team.

A company may also consider alternatives to the Clean Room development process to mitigate the possibility that Outside Protected Information may be used. For example, a company may choose to preemptively instruct employees involved in a development project not to use any third-party information in the course of the development project, or to only utilize information from publicly available sources. A company may also remind its employees that are participating in a development project that those employees have a legal obligation not to use the Outside Protected Information of another company in general or a specific company (e.g., if the employees were previously used in a due diligence project on a particular company). A company may also include provisions in employment agreements informing employees that they are prohibited from using or disclosing any third-party confidential or trade secret information and that they may be subject to repercussions, up to and including termination, for any violations.

Ultimately, a company has a wide variety of safeguards it may choose to employ to either eliminate or at least mitigate the possibility that Outside Protected Information is used in a development project.

3. Individuals who may be involved with monitoring the Clean Room development process

Clean Room development may or may not utilize an entity or person whose job it is to ensure that Outside Protected Information does not enter the Clean Room and/or that the ultimate product of the Clean Room development process did not utilize Outside Protected Information. When used, the "Monitor" will typically have access to all materials in the Clean Room, and among the Monitor's primary responsibilities will be to ensure that the Clean Room does not become contaminated with Outside Protected Information.

In Clean Rooms where a Monitor is used, a subsequent evaluation of that Clean Room development process will likely scrutinize the Monitor, including who served as the Monitor, what the Monitor's role was in the Clean Room development project, and more generally the effectiveness of the Monitor. Where a Monitor is used, in certain circumstances, it may be advisable to hire an independent, third-party Monitor from outside the company who has not had access to the Outside Protected Information and does not have a vested interest in the product that is the subject of the Clean Room development.[4] But in other

4. Resman, LLC v. Karya Prop. Mgmt., LLC, Case No. 4:19-cv-00402, 2021 U.S. Dist. LEXIS 146422, *34 (E.D. Tex. Aug. 5, 2021) (appointing Magistrate Judge as independent monitor); Hologic, Inc. v. Direct Digital Imaging Tech. (Beijing), 2018 Mass. Super. LEXIS 542, *3 (Mass. Superior Court) (appointing Magistrate Judge, who also was tasked with resolving disputes regarding clean room); Bridgetree, Inc. v. Red F Mktg. LLC, No. 3:10-CV-00228-FDW, 2013 WL 443698, at *23 (W.D.N.C. Feb. 5, 2013) (requiring "[a] third party 'gatekeeper,' who is an independent, third party forensic examiner with expertise in source code development and analysis, to be mutually selected by the parties").

situations where a Monitor is used, this may not be practical or necessary.[5]

Where a Monitor is used, the Monitor may screen all communications regarding the Clean Room development going into the Clean Room to ensure they do not contain or reflect Outside Protected Information and/or the Monitor may be copied on all such communications. In situations where the Monitor has received or had access to all communications going into the Clean Room, the Monitor may then be able to attest that no Outside Protected Information was communicated to the Clean Room in any of those communications.[6]

If the Monitor discovers that a communication contains the Outside Protected Information or could be reasonably construed to contain the Outside Protected Information, the Monitor should inform the Manager(s) and/or Clean Team and take steps to ensure that that information is not used or otherwise

5. Nordstrom Consulting, Inc. v. M & S Techs., Inc., Case No. 06 C 3234, 2008 U.S. Dist. LEXIS 17259, at *21-23 (N.D. Ill. Mar. 4, 2008) (not requiring independent monitor, and dismissing concern that the clean room was infected by those with knowledge of the source code at issue stating, "[e]ven if Plaintiffs could establish that the developers of the new software had access to the NCI Software, they would still need to prove that the new software is substantially similar to the NCI Software"); ECIMOS LLC v. Carrier Corp., Case No. 2:15-cv-2726-JPM-cgc, 2019 U.S. Dist. LEXIS 199746, *13 (W.D. Tenn. Aug 15, 2019) (allowing company employee to serve as monitor, under direction of Special Master).

6. Epic Sys Corp v. Tata, Case No. 14-cv-748-wmc, 2016 U.S. Dist. LEXIS 60344. *5 (W.D. Wis. Apr. 27, 2016) ("While plaintiff will be allowed to direct the monitor's activities, consistent with those outlined in the permanent injunction, plaintiff will not be privy to the outcome of that review, except for disclosure of any evidence of a violation of the permanent injunction itself, and defendants may seek relief from the court if they believe the monitor's activities exceed the parameters of the injunction.").

incorporated into the product being developed in the Clean Room.

When a Monitor is used, the Clean Room Protocol should consider including an instruction requiring any communications to the Clean Team to first be screened by the Monitor to verify that the communication does not contain Outside Protected Information before it is sent to the Clean Team. Alternatively, the Protocol may include an instruction that the Monitor be copied on all communications to the Clean Team, as well as an instruction that any inadvertent communication from outside the Clean Room related to development issues will be reported to the Monitor. In either instance, the Monitor may examine the communication to either verify that no Outside Protected Information was shared or, if possible and as necessary, take steps to remediate any sharing of Outside Protected Information.

In situations involving the use of both a Monitor and a Dirty Team to prepare a functional specification that describes the required features of the product that will be developed in the Clean Room, the Monitor may be utilized to review the specification for any Outside Protected Information before it is provided to the Clean Team. If the Monitor determines that the specification does not contain any Outside Protected Information, the Monitor can then transfer it to the Clean Room.

When used to review the specification, if the Monitor finds Outside Protected Information, the Monitor sends the specification back to the Dirty Team to resolve the issue and eliminate any reference to, or disclosure of Outside Protected Information. The Dirty Team will rework the specification and transfer it back to the Monitor until the Monitor verifies it as containing no Outside Protected Information and transfers it to the Clean Room. If the Clean Team has questions, those questions may be

routed through the Monitor first, and the Monitor may be used to review the response from the Dirty Team before it is provided to the Clean Team to ensure it does not divulge any Outside Protected Information.

A Monitor may also be utilized to verify that the final product created in the Clean Room does not contain the Outside Protected Information.

4. Involvement of counsel in the development process

Principle 4: Counsel may be uniquely positioned to consult on the design of the Clean Room and whether the processes for the Clean Room are appropriate in view of the legal landscape, litigation concerns, or other legal concerns the company may have.

Guideline 1: It is often, but not always, necessary for counsel to participate in the Clean Room process. Counsel, both inside and outside, will often play a crucial role in developing and implementing a Clean Room process and may be involved in one or more of the following functions:

- Identification of what information constitutes Outside Protected Information and what information is not Outside Protected Information.
- Identification of individuals who may have had exposure to Outside Protected Information, those individuals who did not have exposure to Outside Protected Information, and, relatedly, those individuals who should or should not have access to the Clean Room.

- Consultation regarding, or the design, preparation and set up of a Clean Room Protocol as well as other legal requirements and considerations for the Clean Room.
- Consultation regarding the product development in the Clean Room itself, *e.g.*, intellectual property counsel may provide freedom to operate advice to the members of the Clean Room in view of public intellectual property rights.
- Consultation regarding, or the implementation of, a Clean Room Protocol.
- Consulting and/or conducting periodic check-ins regarding the progress of Clean Room development and continued need for the Clean Room.
- Serving as, or consulting with the Monitor for the Clean Room, if a Monitor is used, ensuring Outside Protected Information does not go into the Clean Room.
- Consultation regarding, or the implementation of, procedures regarding the Dirty Team.

Counsel also may have responsibilities at the company, such as ethics and addressing potential legal liabilities, which require their involvement in the set up or implementation of a Clean Room. Alternatively, if a Clean Room commences during litigation, litigation counsel may need to be involved, or a court may mandate counsel involvement.

Counsel may also need to be involved in Clean Room development or implementation to ensure that applicable rules and regulations are adhered to during the Clean Room process.

Counsel may also have possession of Outside Protected Information, e.g., part of a team negotiating a failed deal during

which Outside Protected Information was exchanged that the company now wants to avoid using and therefore may need to be screened from the Clean Room development process.

Principle 5: When legal counsel is involved in a Clean Room development process, care should be taken to avoid inadvertent and unintended waiver of privilege or work product protections connected to the involvement of counsel or, if waiver is reasonably foreseeable, measures should be taken to plan and define the scope of the intentional waiver.

Guideline 1: To avoid inadvertent waiver or intentional waiver with an unintended scope, consider whether the role of counsel and what aspects of Clean Room development counsel is working on should be clearly defined and memorialized.

Guideline 2: To avoid inadvertent waiver or intentional waiver with an unintended scope, consider whether to divide responsibilities among separate legal counsel, such as by having one counsel advise on issues where waiver is foreseeable and a separate counsel advise on issues where waiver is not foreseeable.

Since it is often necessary to disclose various details concerning the Clean Room process employed by a company to a tribunal or third party, a company may intentionally or unintentionally waive attorney-client privilege or work product protections

where counsel is involved in the Clean Room process.[7] Therefore, parties seeking to utilize a Clean Room must exercise care and consider whether and how to structure attorney involvement in the Clean Room process from the outset to avoid unintentional waiver or limit the scope of an intentional waiver.

Certain courts have held that where an attorney has communications with employees in a "Clean Room" during a development process, those communications may be "at issue" and therefore discoverable. Indeed, the communications may be determined to be "at issue" if the party challenging the Clean Room can show that it needs those communications to evaluate the effectiveness of the Clean Room.[8]

Similarly, other courts have indicated that where an attorney with knowledge of the Outside Protected Information is the Monitor, that attorney's communications with the Clean Room are not protected by attorney-client privilege.[9]

Courts may also reach different conclusions on whether legal advice related to the design of a Clean Room and product development in a Clean Room is protected or at issue, which may depend on what happens during litigation. For example, earlier drafts of a Clean Room Protocol reflecting legal advice may be protected from disclosure where a party challenging the Clean Room is unable to show a need for those earlier privileged

---

7. *See, e.g.*, Cargill Inc. v. Budine, No. CV-F-07-349- LJO-SMS, 2008 U.S. Dist. LEXIS 72809, at *10 (E.D. Cal. July 21, 2008) (finding subject matter waiver for communications regarding clean room).

8. See Computer Associates Intern. v. Quest Software, Inc., 333 F. Supp. 2d 688, 701 (N.D. Ill. 2004).

9. *See* Brocade Commc'ns Sys., Inc. v. A10 Networks, Inc., Case No. 10–CV–03428–LHK, 2013 U.S. Dist. LEXIS 18870, at *38-39 (N.D. Cal. Feb. 12, 2013) (attorneys with knowledge of the trade secrets can be appointed as monitor, even though it may waive privilege in certain circumstances).

drafts of the Clean Room Protocol. On the other hand, if counsel advises on freedom to operate or noninfringement of patent rights during the Clean Room development process, and if a company later affirmatively relies on that advice in a subsequent proceeding, privilege as to that advice will likely be found waived and the extent of that waiver may be hard to anticipate in advance.

To mitigate the risk of inadvertent waiver or intentional waiver with an unintended scope, companies should clearly define and memorialize in writing the role and responsibilities of counsel in the Clean Room development process. Companies may also consider structuring counsel involvement in a Clean Room development process, e.g., by using different counsel to perform different functions, based on how they intend to use the Clean Room and based on whether they may need to place certain communications involving counsel at issue to the extent the Clean Room is later the subject of litigation. For example, if the Monitor for the Clean Room is an in-house attorney, a company may wish to have a different in-house attorney or any outside attorney advise the development team on freedom to operate related to patent rights held by third parties.

D. Involvement of Artificial Intelligence Tools

Clean Room development may be aided by using artificial intelligence (AI) tools. Depending on how such tools are used, this could have the benefit of accumulating all available information to the Clean Room participants without human involvement or intervention, potentially lowering the possibility of human-created issues such as contamination between the Clean Room and the Outside Protected Information, bias or error. This assumes, however, that the AI tools are properly developed and customized, and that they were not themselves trained with any Outside Protected Information.

E. Preparing a Clean Room Protocol

Principle 6: A Clean Room Protocol should clearly describe the restrictions put in place to prevent the Clean Team from using or incorporating Outside Protected Information in product development.

In implementing a Clean Room, it is recommended that the Clean Room procedures be documented in a Clean Room Protocol. The Protocol is designed to ensure that (1) exposure to Outside Protected Information by those in the Clean Room is extremely unlikely if not impossible and (2) a subsequent evaluator (e.g., judge or jury) would understand that from reviewing the protocol. The Clean Room Protocol is to be shared with everyone involved in the Clean Room project: the Clean Team, the Dirty Team (if any), the Monitor (if any), and any other relevant employees as necessary or appropriate for the particular Clean Room project (e.g., project managers, administrative staff, executives, etc.).

Note that while the following discussion of the elements that may be included in a Clean Room Protocol contains recommended guidelines, these are not exclusive and other methodologies not described herein can also be used by an organization to protect against the disclosure or use of Outside Protected Information. The company developing the new product should seek advice from competent lawyers and business advisors about its specific situation and requirements. Again, the use of or failure to utilize any of the recommended guidelines discussed herein is not dispositive of the effectiveness of any Clean Room development project.

Whether a particular Clean Room implements more or less stringent measures may depend on several factors,[10] including the goal(s) of the Clean Room; the industry[11]; the physical, financial, and practical limitations of the particular company in question; the specific development at issue; and other factors. As one court has explained, however, a Clean Room "is a valuable exercise only if procedures are followed to make certain that no improper material passes through the walls."[12]

The Clean Room Protocol may include the following:

- A description of the reason for, or purpose of implementing the Clean Room;
- The physical location of the Clean Room and/or Dirty Room (if applicable) and access control measures, if any;
- The virtual location of the Clean Room and/or Dirty Room (if applicable) and access control measures, if any;

10. *See* Miller UK Ltd. v. Caterpillar, Inc., No. 10-CV-03770, 2015 WL 10818831, at *6-7 (expert opinion excluded on question of whether "clean room design was necessary or appropriate *under the circumstances*" (emphasis added)).

11. *See, e.g.*, Comet Techs. USA Inc. v. XP Power LLC, No. 20-CV-06408-NC, 2022 WL 2442810, at *2 (N.D. Cal. Mar. 2, 2022) (expert opinion on "an industry standard of clean room procedures to separate employees hired from competitors").

12. Computer Assocs. Int'l v. Quest Software, Inc., 333 F. Supp. 2d 688, 701 (N.D. Ill. 2004); *cf*. UPI Semiconductor Corp. v. Int'l Trade Comm'n, 767 F.3d 1372, 1381-82 (Fed. Cir. 2014) (even where accused company "took steps to insulate its new product lines from any misconduct that took place in the past" and "engaged outside design firms to create new layouts and schematics," its efforts were insufficient to qualify as a trade secret clean room in light of evidence of contamination).

- Identification of the Outside Protected Information that should not be disclosed to the Clean Team;
- Identification of the individuals who are on the Clean Team;
- Identification of individuals who have had exposure to Outside Protected Information and/or the Dirty Team, if any;
- Identification of the Manager and/or Monitor(s), if any;
- Instructions and procedures to be followed throughout the Clean Room development process;
- Identification of any documents or materials to be provided to the Clean Team and/or the Dirty Team (if any), such as a specification;
- An instruction to raise any issues regarding the Clean Room Protocol promptly; and
- Signed assurance/affirmation by each relevant person that the person will comply with the Protocol.

1. Purpose Description

Guideline 1: To enable participants and evaluators of a Clean Room to understand the purpose of the Clean Room development, it may be helpful for the Protocol to set forth a description of the purpose of the Clean Room.

The purpose of the Clean Room development should usually be well defined from the beginning so that all participants understand what the goal is. Many employees may be unfamiliar with what a Clean Room is or why it is being implemented. It is usually recommended that the Protocol describe, at a high level,

what a Clean Room is and the specific facts for why the company is implementing the Clean Room in a particular situation.

For example, the Protocol might explain that certain employees at the company had access to a competitor's Outside Protected Information as part of a license agreement that is expiring; rather than renewing the license, the company has decided to develop its own competing technology internally. To protect its innovations and guard against the risk of intellectual property claims from the competitor, the company has decided to implement a Clean Room development process whereby the employees working on the development of the new technology will not have any exposure to the competitor's Outside Protected Information.

As another example, the Protocol might explain that there is a dispute with a third party as to whether the company has the right to use certain information or the scope of the company's rights to use certain information. In such circumstances, the Protocol may explain that, out of an abundance of caution and to avoid or minimize disputes, the company has decided to implement a Clean Room development process.

2. Identification of the Outside Protected Information

Guideline 2: To allow relevant individuals to identify the Outside Protected Information that should not be used by the Clean Team, consider whether the Protocol should describe, without disclosing, the Outside Protected Information.

To ensure there is no confusion about what is or is not allowed in the Clean Room, it is usually recommended that the Protocol identify the Outside Protected Information at issue. This should be done in a sufficient level of detail so the relevant

individuals are able to identify the Outside Protected Information that should not be accessed by the Clean Team, but without disclosing the Outside Protected Information in the Protocol itself.

For example, using the same example as above, the Protocol might include the definition of "Confidential Information" as used in the license agreement and/or identify the specific types or categories of Outside Protected Information belonging to the competitor to which the company had access in the ordinary course of the licensing relationship to which it no longer has rights.

3. Identification of Clean Room Participants

Guideline 3: To maintain an accurate record of Clean Room participants and facilitate compliance with the Clean Room Protocol, consider whether the Protocol should identify the individuals on the Clean Team, any individuals with exposure to or familiarity with the Outside Protected Information (such as those on the Dirty Team), the Manager(s), and/or any Monitor of the Clean Room.

a. Identification of Clean Team

The Protocol should usually identify, by name, the individuals who are on the Clean Team. If additional individuals are added to the Clean Team or members are removed, the Protocol should be updated accordingly and note the dates when each person joined or was removed.

Consideration may be given to requiring Clean Team members in particular situations to complete questionnaires

concerning exposure to protected materials in order to establish their lack of exposure. For example, a questionnaire could more specifically probe an individual's prior work history with particular industry standard technologies and/or competitor-specific technologies (without disclosing the confidential details of such competitive technologies). Experience with the former could be beneficial to support a demonstration of independent development, while experience with the latter may counsel in favor of excluding the individual from the Clean Room development.

b. Identification of Individuals with Exposure to Outside Protected Information and/or the Dirty Team

As noted above, individuals at the company with exposure to or familiarity with Outside Protected Information should not be on the Clean Team. In addition, where a Dirty Team is utilized, the Protocol should usually identify, by name, the individuals who are on the Dirty Team; if additional individuals are added to the Dirty Team or members are removed, the Protocol should be updated accordingly and note the dates when each person joined or was removed.

c. Identification and Role of the Monitor

If a Monitor is used, the person or persons designated as Monitors should usually be identified, by name, in the Protocol. If an outside company is designated as a Monitor, only specific employees of that company should be allowed to act as Monitors, and those persons should be named in the Protocol. Any people who are subsequently designated as Monitors or who are removed as Monitors should be noted in the Protocol, along with the dates when each person became or ceased being the Monitor. The role of the Monitor may be discussed in the

Protocol, including the mechanisms employed by the monitor—e.g., reviewing materials before they can be shared with a clean team; monitoring only between specific members of the development team; or periodic monitoring or testing of development documents for contamination.

The benefit of having an outsider as the Monitor is that they can be truly independent. Indeed, some courts have appointed a neutral, or even a magistrate judge, to oversee clean rooms. This removes any potential bias towards the company whose technology is being monitored. The downside of having an outsider is that although the outsider may have familiarity with the legal aspects of the case, s/he may not be as familiar with the technology and therefore may not recognize what is or is not Outside Protected Information.

The benefit of having an insider, such as an attorney or an engineer, as the Monitor is that they are likely to have better familiarity with the at-issue technology and thus an enhanced ability to keep out Outside Protected Information. They are also more likely to be familiar with the company's documents, data and procedures. The downside of having an insider as the Monitor is that they may be biased—or be perceived as being more biased—towards the company whose technology is being monitored, whether expressly or implicitly.

4. Clean Room Protocol Instructions and Procedures

Guideline 4: To ensure that Clean Room participants understand their obligations and the procedures to be followed under the Protocol, consider whether the Protocol should contain clear instructions and procedures for the Clean Room and whether the Company

should maintain records of such instructions and procedures.

The Clean Room Protocol instructions and procedures may include the following:

a. Instructions to the Clean Team

This section of the Protocol gives the Clean Team the specific instructions and procedures they are to follow in connection with the Clean Room development project—*i.e.*, the dos and don'ts. For example, instructions and procedures may include:

- Do not ask others who have had exposure to the Outside Protected Information to disclose Outside Protected Information or otherwise disclose any information about the Outside Protected Information;
- Keep a log of resources used or consulted—for example, keep a list of any documents provided to the Clean Team, any articles relied upon, and any products to which the Clean Team had access for purposes of reverse engineering (including when and how those products were obtained, receipts, etc.). To the extent that the company's ordinary development process is already documented using standard application development procedures that are themselves documented, trained on, and monitored for compliance, this step may be redundant.
- Follow the established communication methods and procedures (see below).
- Prepare periodic reports on the development timeline and progress (see below).

It may be helpful to conduct training on the Clean Room Protocol instructions and procedures for the Clean Team. The training may include an opportunity for members of the Clean Team

to seek clarification on aspects of the instructions and procedures, either during the training or later during the development process.

b. Instructions to the Individuals with Access to Outside Protected Information and/or the Dirty Team (if any)

This section of the Protocol gives any individuals who have or have had access to Outside Protected Information specific instructions and procedures they are to follow in connection with the Clean Room development project—*i.e.*, the dos and don'ts. For example, instructions and procedures may include:

- Do not disclose Outside Protected Information or any information about the Outside Protected Information to the Clean Team;
- Keep a log of resources used or consulted—for example, keep a list of any Outside Protected Information provided to the Dirty Team and any products to which the Dirty Team had access for purposes of reverse engineering (including when and how those products were obtained, receipts, etc.).
- Follow the established communication methods and procedures (see below).
- Keep a log of any materials provided to or communications with the Clean Team (if any).

c. Periodic Reports

In certain circumstances, the Clean Team may be required to prepare regular reports on its activities, for example, if the Clean Room is required by a court order or where the organization requires periodic progress reports or deems such reports advisable under the circumstances. If the Clean Team is instructed to

prepare regular reports on its activities, the Protocol can specify the format and frequency of those reports, who is responsible for preparing the reports, to whom the reports should be submitted, and, depending on the circumstances, generally what type of information should be included in the periodic report.

d. Location of the Clean Room and/or the Dirty Room

The Protocol can explain that a "Clean Room" is a place—that may or may not be an actual, physical room or space—where developers, scientists, and other employees have no exposure to any materials that contain or could contain the Outside Protected Information.

In certain situations, the Clean Room may be a physical space where access can be monitored and verified—for example, a room that can be accessed only by certain authorized personnel with a keycard or other system that tracks entry and exit. When a physical space is utilized, consider specifying in the Protocol the location of the Clean Room and including instructions around access restrictions, etc. In other situations, there may be no separate "room" at all, and the term "Clean Room" is simply a metaphor for a development process that is clean from Outside Protected Information.

Similarly, in situations where the Clean Room development project involves a Dirty Team, there may be an actual, physical room or space—the "Dirty Room." Again, where used, the location of the Dirty Room should usually be specified in the Protocol and should be in a different location from the Clean Room.

The Protocol may identify virtual locations (e.g., network folders, databases) where developers, scientists, and other employees may access any materials to be used for the Clean Room development. When virtual locations are utilized, the Protocol

should usually specify those locations and include instructions regarding such locations, such as access restrictions.

Similarly, in situations where the Clean Room development project involves a Dirty Team, there may be virtual locations identified to house Outside Protected Information. Where used, the virtual locations of the Outside Protected Information may be specified in the Protocol and should usually be in a different location than the virtual Clean Room development materials. Clean Team members should not have access to the virtual locations of the Outside Protected Information, and access should be monitored as needed.

e. Communications methods and procedures

This section of the Protocol should usually specify any instructions regarding communications to or from the Clean Team. It should usually specify *how* communication is to take place and/or any restrictions on the methods of communication that are allowed—e.g., hardcopy documents, email, flash drives or other removable drives, collaboration software (e.g., MS Teams, Slack), etc. It should also usually specify *whether* communications may be made directly to the Clean Team or, in situations where a Monitor is used, if the Monitor must be copied or if any communications must first be screened by the Monitor before being passed to the Clean Team. And it should usually specify what information should be included in any communication—e.g., to clearly identify or label the communication as relating to the Clean Room development project.

To the extent any individuals with access to Outside Protected Information and/or the Dirty Team have communications with the Clean Team (directly or through a Monitor), it is usually recommended that instructions be given about the dos and

don'ts of the content of those communications. Such instructions may include, for example:

- Provide only high-level specifications or business requirements to the Clean Team that do not disclose Outside Protected Information or any information about the Outside Protected Information;
- Keep a log of any communications or information provided to the Clean Team, including the date and content of the communication, and to whom and from whom it was sent. To the extent that the company's ordinary development communications are already documented using specific means (e.g., ticketing system) via standard application development procedures that are themselves documented, trained on, and monitored for compliance, this step may be redundant. Further, to ensure such communications are properly maintained, consider establishing a minimum length of time for archiving that may exceed the company's standard documentation practices.
- Any communication with or information provided to the Clean Team may be closely scrutinized if the Clean Room is later challenged, for example, in any subsequent litigation. For that reason, it is usually recommended that any such communications be kept to a minimum and that care is taken to ensure that no Outside Protected Information is disclosed (inadvertently or otherwise).

f. Identification of Documents and Materials

It is usually recommended that the Protocol list those documents and materials that will be provided to the Clean Team and Dirty Team (if any), including any hardware or software.

Any documents discovered later or determined to be necessary during the development procedure should usually be added to this list.

g. Instruction to Raise Issues

The Protocol should usually be set up so that any violations, while not impossible, would almost certainly be noticed and recorded so that steps to remediate those violations could be taken. To this end, those involved in the Clean Room development process should be instructed to raise any issues or potential issues immediately. For example, the Protocol may state: "If you realize at any point that you or another member of the Clean Team have had exposure to Outside Protected Information, notify [insert contact person] immediately."

If an issue is raised, the Monitor or others should determine whether any Outside Protected Information was disclosed to the Clean Team. If so, the company may need to determine how best to resolve the situation, which may depend on the specific facts of the situation, including the type of disclosure, to whom the disclosure was made, the purpose of the Clean Room,[13] etc. Resolutions may include, for example:

- Removing certain individuals from the Clean Room development project who have violated the Protocol;
- Removing certain individuals from the Clean Team if they have been exposed to Outside Protected Information; or

13. For example, in the case of a court-ordered clean room, the fact of the disclosure of Outside Protected Information may need to be communicated to a judicial officer to determine the appropriate remedy.

- Issuing instructions to the Clean Room on how to not use the Outside Protected Information and/or how to remedy any taint.
- Quarantining the relevant documents and information.
- Taking other measures to ensure and to document that the Outside Protected Information was not further used or incorporated into any products.
- Terminating the Clean Room development project and starting the process over from the beginning with a new Clean Team.

Considerations of what resolution(s) to use may include the following:

- Whether Outside Protected Information was used by the Clean Team, and whether that information truly is trade secret or confidential or instead was kept from the Clean Team only out of an abundance of caution;
- Whether the Dirty Team communicated directly or indirectly with the Clean Team, and the nature of the communication;
- Whether any Outside Protected Information that was used affects the entire project, or only a separable portion of the project;
- How far along the project is and how important the Outside Protected Information was to the development; and
- The purpose of the Clean Room

5. Signed Assurance/Affirmation

Guideline 5: To document that Clean Room participants and other relevant individuals will comply with the Protocol, consider whether the Protocol should include a signed acknowledgement.[14]

It is usually recommended that everyone involved in the Clean Room project sign agreements not to violate the Protocol and to commit to following the documented procedures. This includes everyone on the Clean Team, the Dirty Team (if any), the Monitor (if any), and any other relevant employees as necessary or appropriate for the particular Clean Room project (*e.g.*, project managers, administrative staff, executives, etc.). All people involved should understand the importance of the development project and the seriousness of the endeavor. They should also be advised that violations of the procedures may have serious consequences.

In addition, at the end of the Clean Room project, consider whether to have everyone involved in the Clean Room project attest that they have not used any Outside Protected Information. In some circumstances, a company may also wish to obtain signed attestations from employees *outside* the Clean Room, saying that they did not give any Outside Protected Information to the development team. In addition, if an employee involved in the Clean Room project gives notice that he or she intends to leave the company prior to the end of the Clean Room project, a

14. *See, e.g.*, Bridgetree, Inc. v. Red F Mktg. LLC, No. 3:10-CV-00228-FDW, 2013 WL 443698, at *23–24 (W.D.N.C. Feb. 5, 2013) (specifying that only employees and agent who had no exposure to the trade secret would be allowed to enter the clean room, also requiring that they read the court order and sign an affidavit that they would comply).

company may also wish to obtain a signed attestation from that employee prior to his or her departure confirming that that employee did not use Outside Protected Information during the course of his or her participation in the Clean Room project.

APPENDIX A: SAMPLE CLEAN ROOM PROTOCOL[15]

Clean Room Protocol for Development of [Insert Description]

Date:

To: Recipients ("Clean Team"):

List full name of all recipients—i.e., the "Clean Team"

Purpose of Protocol and Identification of Outside Protected Information:

As you know, [Company] is planning to develop its own [insert description], without relying on, using, or referencing any confidential or trade secret material from outside [Company] to which [Company] does not have rights [or to which [Third Party] has alleged [Company] does not have rights] (hereinafter "Outside Protected Information"), including but not limited to any Outside Protected Information [Company] may have obtained or had access to from [Third Party]. The purpose of developing [insert description] in a Clean Room environment is to protect [Company's] innovations and minimize the risk that [Third Party] could argue that [Company] infringed its intellectual property [and/or violated the terms of its contract with

15. This Sample Clean Room Protocol represents WG12's views about certain aspects of clean room development, including when a Protocol may be provided, what a Protocol may contain, and how a Protocol may be tailored to the specific development process at issue. The Sample Clean Room Protocol is not intended to state or displace current law regarding clean rooms, which is developing and often fact dependent and thus does not lend itself to the development of more authoritative Best Practice recommendations. Rather, the Sample Clean Room Protocol is intended to constitute a practical example of WG12's consensus Principles and Guidelines regarding such a protocol. In certain circumstances, it may also be appropriate to put a similar protocol in place for the "Dirty Team" or "Specification Team" as described above in Part III.C.2.

[Third Party]]. This document describes a protocol to implement and operate such a Clean Room.

[If contractual restrictions are at issue, relevant provisions may be included in the Protocol and/or an appendix to the protocol—e.g.:

[Company's] contract with [Third Party] prohibits [Company] from, among other things, copying, altering, decompiling, reverse engineering, disassembling, or creating derivative works from [Third Party's] [product—e.g., "software," "hardware," "technical documentation," etc.]. In short, [Company] cannot use [Third Party's] [product] to develop [insert description]. A copy of the relevant provisions of [Company's] contract with [Third Party] are attached as Exhibit A to this Protocol.]

or

[Third Party] disclosed certain Confidential Information to [Company] pursuant to the [contract]. [Company's] contract with [Third Party] defines "Confidential Information" as [insert definition].]

[Where contractual restrictions are not at issue, a description of the Outside Protected Information that does not disclose any protected details of the information itself may be included in the Protocol and/or an appendix to the Protocol—e.g.:

Company is prohibited from using certain chemical combinations developed by competitor [*insert name*] for improving jet fuel burn rates.]

Procedures:

Below are instructions and procedures to help ensure and demonstrate that [Company's] development efforts are independent of any [Third-Party] Outside Protected Information. In general, the Clean Team's development activities should be independent from activities of any [Company] employees who

may have had exposure to any [Third-Party] Outside Protected Information.

[*Include as applicable*: Team Members: Specification Team

You will be provided with a Specification to assist the Clean Team in developing [insert description]. The Specification will describe the required features of the product that will be developed in a way that does not use, contain, or disclose any Outside Protected Information. The following individuals were involved in developing the Specification:

List full name of all participants.]

Team Members: Clean Team

Prior to any involvement with the Clean Team, all Clean Team members must have signed non-disclosure/confidentiality agreements with the Company. No persons who have had exposure to any [Third-Party] Outside Protected Information shall have any involvement with the Clean Team's development activities.

[*Include as applicable:* The following persons may have had exposure to [Third-Party] Outside Protected Information: [insert list of full names or append as Exhibit].]

Do not ask anyone who may have had exposure to Outside Protected Information to disclose Outside Protected Information to you or otherwise disclose any information about the Outside Protected Information to you.

The Manager(s) will manage and supervise the entire Clean Room setup process. The Manager(s) shall be [name and contact information].

[*Include as applicable:* The Manager shall be accountable for the Clean Room development process.]

[*Include as applicable:* The Monitor is responsible for screening communications with and between members of the Clean

Team to avoid contamination [OR to ensure they do not contain or reflect Outside Protected Information]. [AND/OR The Monitor is responsible for reviewing the Specification before it is provided to the Clean Team to ensure it does not contain or reflect Outside Protected Information]. The Monitor shall be [name and contact information].]

Record Keeping and Use of Materials

Keep records of the independent development.

[*Include as applicable*: The following materials will be provided to you and may be used by you during the Clean Room development process: [insert list and update as needed].]

[*Include as applicable*: Only materials in Appendix [__] to this Protocol may be provided to the Clean Team.]

Keep a log of resources used or consulted during the Clean Room development process—for example, keep a list of any documents provided to the Clean Team, any articles consulted, and any products to which the Clean Team had access for purposes of reverse engineering (including when and how those products were obtained, receipts, etc.). The documentation should include as much detail as feasible about the individuals involved, the products and processes developed (including when and where such products and processes were developed), and all sources of information.

[*Include as applicable*: Ordinary application development procedures should be used to document resources used or consulted during the Clean Room development process.]

[*Include as applicable*: Clearly mark the documents used as part of the Clean Room development process.]

Keep records of instructions given to the Clean Team.

[*Include as applicable:* Keep all communications or information provided to the Clean Team, including the date and content of the communication and who it was sent from and to.]

[*Include as applicable*: To the extent that the company's ordinary development communications are already documented using specific means (e.g., ticketing system) via standard application development procedures that are themselves documented, trained on, and monitored for compliance, you may rely on such processes to document Clean Room development.]

[*Include as applicable*: To ensure Clean Room development communications are properly maintained, such communications shall be maintained through archiving for [insert a minimum length of time that may exceed the company's ordinary documentation practices].]

Physical/Virtual Spaces

[*Include as applicable*—i.e., when using a separate physical space for Clean Room development: The Clean Room shall be located in [___].

[*Include as applicable:* The Clean Room may be accessed only using keycards. No piggybacking on keycard access shall be permitted.]

[*Include as applicable:* Members of the Specification Team shall not have access to the Clean Room.]

[*Include as applicable:* No Outside Protected Information should be brought into the Clean Room [AND/OR] no resources may be brought into the Clean Room without the approval of the Monitor.]

[*Include as applicable*: Resources used or consulted during the Clean Room development shall not be removed from the Clean Room.]

[*Include as applicable*: A separate Dirty Room which may contain documents, data, and other information used to develop [interface/competing technology/etc.] shall be located at [___].]

[*Include as applicable:* The Dirty Room may be accessed only using keycards. No piggybacking on keycard access shall be permitted.]

[*Include as applicable:* Members of the Clean Team shall not have access to the Dirty Room.]]

[*Include as applicable—i.e., when using virtual security measures*: The Clean Team virtual development resources shall be located at [___].

[*Include as applicable:* Access to Clean Team virtual development resources shall be controlled by [Manager/Monitor/dedicated IT resource].]

[*Include as applicable:* The names of individuals who are granted access to Clean Team virtual development resources shall be kept on access control lists.]

[*Include as applicable:* Access to Clean Team virtual development resources shall be periodically monitored by [Manager/Monitor/dedicated IT resource].]

[*Include as applicable:* Access to Clean Team virtual development resources shall be periodically audited by [Manager/Monitor/dedicated IT resource].]

[*Include as applicable:* Clean Team members must not access (or have the ability to access) any electronic data sources containing Outside Protected Information.]

[*Include as applicable:* No Outside Protected Information should be placed into the Clean Team virtual development space(s) or electronic resources [AND/OR] no resources may be placed in the Clean Room development virtual space(s) or electronic resources without the approval of the Monitor.]

[*Include as applicable*: Resources used or consulted during the Clean Room development shall not be removed from the Clean Room development virtual space(s) or electronic resources.]

[*Include as applicable:* Separate Dirty Room development virtual space(s) or electronic resources which may contain documents, data, and other information used to develop [interface/competing technology/etc.] shall be located at [___].]]

Communications

[*Include as applicable*: Any communications between the Clean Team and the Specification Team must be in writing.]

[*Include as applicable*: and must be made first to the Monitor, who may modify such written communications before transmission to the intended recipient].]

Reporting

[*Include as applicable*: Prepare [periodic/daily/weekly/other] written reports on the development timeline and progress.

[Manager] shall be responsible for preparing such reports.

[*Include as applicable:* Such reports should be sent to the Monitor via email.]]

If you realize at any point that you or another member of the Clean Team have had exposure to Outside Protected Information or that any of the procedures in this document are not being followed, notify [insert contact person] immediately.

Contact [insert Manager(s) name and phone number] if you have any questions or concerns.

Signed Assurance/Affirmation

This acknowledgement is to be signed and returned to [insert contact name] upon receipt and review of the forgoing

Clean Room Protocol for Development of [Insert Description] (the "Protocol").

By signing below, I hereby affirm and acknowledge that I understand the instructions set forth in the Protocol and agree to abide by them. I further affirm that I have not had exposure to any [Third-Party] Outside Protected Information as of the date of my signature below. If I have any questions or if I realize at any point that I have had exposure to, or learned confidential information about, [Third-Party] Outside Protected Information, I will immediately notify [insert contact name and phone number].

[*Include as applicable*: I understand that if I violate the Protocol or refuse to comply with reasonable instructions from the Monitor or Manager, I will be subject to disciplinary action, up to and including termination of my employment, and may face further legal action as appropriate.]

Employee Signature: _____

Employee Name: _____

Date: _____

RETHINKING NEGLIGENCE CLAIMS IN CYBERATTACK CLASS ACTIONS: TEACHINGS OF THE THIRD TORTS RESTATEMENT REGARDING ACTIONABLE INJURY

By Douglas H. Meal

Mr. Meal is an Adjunct Professor at Cleveland State University College of Law and Boston College Law School. He teaches Cybersecurity Litigation at each institution. The views expressed in this article are his own and are not attributable to either institution with which he is affiliated. Nor do they necessarily represent official positions of The Sedona Conference.

Mr. Meal acknowledges with deep thanks the invaluable assistance of his Research Assistants, Ms. Kyndal N. Hutchison and Ms. Taneisha M. Fair, each of whom is a 2025 graduate of Cleveland State University College of Law, and Ms. Amanda Borngen, a member of the class of 2026 at Cleveland State University College of Law, in the preparation of this article.

This publication may be cited as follows:

> Douglas H. Meal, *Rethinking Negligence Claims in Cyberattack Class Actions: Teachings of the Third Torts Restatement Regarding Actionable Injury*, 26 SEDONA CONF. J. 357 (2025).

TABLE OF CONTENTS

INTRODUCTION

Cyberattacks that target personal information have, unfortunately, become a normal part of everyday life in the 21st century. Just as ubiquitous, at least in the United States, are the class action litigations that inevitably ensue from such cyberattacks. Normally, though not invariably, such class actions are filed against the entity that suffers such a cyberattack, on behalf of the individuals whose personal information was involved in the attack. Cyberattack class actions of this particular sort are the focus of this article.

Cyberattack class action complaints often assert a wide range of differing theories of liability against the cyberattack victim. For example, the consolidated class action complaint filed against UnitedHealth Group, whose affiliate, Change Healthcare, suffered one of the most highly publicized cyberattacks during 2024,[1] advances no fewer than 41 different theories of liability in its 41 separate counts.[2] There is one constant: nearly every cyberattack class action complaint, usually in its very first count, alleges a claim against the cyberattack victim based on common-law negligence.[3]

---

1. C. Snowbeck, *1 in 2 Americans affected by UnitedHealth cyberattack, new disclosure shows*, MINNEAPOLIS STAR-TRIBUNE, Jan 25, 2025 ("'Change Healthcare has determined the estimated total number of individuals impacted by the Change Healthcare cyberattack is approximately 190 million,' UnitedHealth Group said in a statement issued Friday afternoon."), available at www.startribune.com/1-in-2-americans-affected-by-unitedhealth-cyberattack-new-disclosure-shows/601210911.

2. *See* Class Action Complaint (Docket No. 1), Christensen v. UnitedHealth Group Inc., No. 0:25-cv-183 (D. Minn. filed Jan. 15, 2025) (hereinafter "UnitedHealth Complaint"), at Counts I-XLI.

3. *See*, e.g., *id*., at Count I.

Cyberattack class action complaints also frequently assert, and seek relief for, a wide range of injuries that the named plaintiff(s) and the members of the putative class allegedly incurred by reason of the cyberattack in question. This article focuses on whether the injuries typically alleged in a cyberattack class action constitute *actionable injury* sufficient to sustain a claim against the cyberattack victim based on common-law negligence.[4] Part I of this article shows that, to date, the courts of the United States have failed to answer this question coherently. They have employed differing analytical frameworks, and arrived at disparate conclusions, regarding what sorts of cyberattack-caused injuries are actionable in negligence. Part II of this article argues that the American Law Institute's ongoing project to replace the *Restatement (Second) of Torts*, by means of its *Restatement (Third) of Torts* series, offers the U.S. courts a common doctrinal basis by which to analyze, and thereby come to consistent answers to, this question: namely, via the principles regarding actionable injury in negligence set forth in the recently finalized *Liability for Economic Harm* and *Liability for Physical and Emotional Harm* parts of the *Restatement (Third) of Torts* series. Part II of this article further shows how application of those principles to the injuries typically alleged in a cyberattack class

4. Defendants in cyberattack class actions often contest whether the complaint's injury allegations are sufficient to give the named plaintiff(s) Article III standing to assert the complaint's claims in federal court. The issue of *standing-creating* injury in cyberattack class actions is not the focus of this article. However, as will be seen, U.S. courts occasionally conflate the issue of whether an alleged injury is *standing-creating* for Article III purposes with the issue whether the injury is *actionable* in common-law negligence, so this article does address the issue of standing-creating injury for the limited purpose of addressing the courts' confusion as to the distinction between an injury that is standing-creating as an Article III matter and an injury that is actionable as a matter of common-law negligence. *See infra* note 49.

action would result in such alleged injuries being found non-actionable in common-law negligence. The article therefore concludes that, if and when the U.S. courts come to follow the *Restatement (Third) of Torts* series, and in particular the series' principles regarding actionable injury in common-law negligence, claims based on common-law negligence should, and will, cease to be viable in cyberattack class actions.

I. THE INCOHERENCE OF THE U.S. COURTS' RULINGS TO DATE REGARDING WHAT INJURIES TYPICALLY ALLEGED IN A CYBERATTACK CLASS ACTION ARE ACTIONABLE IN NEGLIGENCE

Cyberattacks that target individuals' "personal information"[5] are daily occurrences in the United States and around the world. And like night follows day, when a cyberattack involves the personal information of a significant number of United States residents, class action litigation follows like clockwork in the United States.

Typically, cyberattack class action plaintiffs claim that they and the members of the class they propose to represent have suffered, or are at risk in the future of suffering, a wide assortment of injuries by reason of the cyberattack in question. The injury allegations in the recently filed class action complaint in the *UnitedHealth* cyberattack class action are illustrative:

"Plaintiffs have experienced extensive harms as a result [of the cyberattack suffered by Change Healthcare], including, among other things: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft

5. Throughout this article, the term "personal information" is used in its broadest sense, i.e., to mean "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual." *See, e.g.*, Cal. Civ. Code 1798.80(e) (so defining term "personal information" for purposes of California Consumer Records Act).

from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; (9) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (10) a continued substantial and imminent risk of the misuse of their Personal Information."[6]

As this example illustrates, the injuries typically alleged in cyberattack class actions all fall into one of two categories:

Economic injuries: For purposes of this article, "economic injuries" are injuries with respect to which a market exists (at least allegedly) and that therefore can be valued by reference to the market valuation.[7] Lost income, out-of-pocket expenses, loss of business or employment opportunities, overcharges and underpayments, and all other market-measurable injuries of a pecuniary nature, are "economic" injuries.[8] Injuries of this sort are exemplified by Items (3), (4), and (5) of the *UnitedHealth* injury allegations, by the "expense" component of Item (9) of those allegations, and, where they are alleged to have caused the plaintiff a lost economic opportunity measurable by reference to a market valuation, Items (7) and (8) and the "non-expense" component of Item (9). Another injury of this sort is the plaintiff's alleged "lost benefit of bargain" by reason of the failure of the

6. UnitedHealth Complaint, *supra* note 2, 15.

7. *See* Restatement (Third) of Torts: Apportionment of Liability (Am. L. Inst. 1998) (hereinafter "Apportionment of Liability Restatement"), § E18, comment c (defining "economic damages").

8. *See id*. (listing examples of "economic damages").

entity that suffered the cyberattack to provide the promised or otherwise legally required security for the personal information involved in that attack, the theory being that because of such failure the plaintiff either (a) overpaid for a product or service he or she purchased from that entity[9], or (b) was under-compensated for employment services he or she rendered to that entity.[10]

Non-economic injuries: For purposes of this article, "non-economic injuries" are all alleged injuries that are not "economic injuries" as defined above. In the cyberattack context, non-economic injuries are invariably intangible in nature[11]; as such, they have economic value both to those who suffer them and in sound economic analysis, but they are not susceptible to market

9. *See, e.g.*, Complaint (Docket No. 1), Washburn v. CPS Solutions, LLC, Case No. 2:25-cv-00400, ¶ 108 (S.D. Ohio filed Apr. 14, 2025) (hereinafter "CPS Solutions Complaint") (alleging lost benefit of the bargain on an overpayment-for-services theory of this sort).

10. *See, e.g.*, Complaint (Docket No. 1), Hamlin v. OBI Seafoods, LLC, Case No. 2:25-cv-00618, ¶ 120 (W.D. Wash. filed Apr. 7, 2025) (hereinafter "OBI Seafoods Complaint") (alleging lost benefit of the bargain on an under-compensation theory of this sort).

11. Bodily harm is the principal tangible injury that at least in most contexts would be non-economic under the definition employed here, see Restatement (Third) of Torts: Remedies (T.D. No. 2 2023) (hereinafter "Remedies Restatement") § 20, comment d), but bodily harm is never an alleged injury in a cyberattack class action. Physical injury to tangible property is the other tangible injury that, at least in some circumstances, could potentially be considered non-economic under the definition employed here, *see id.* (noting that "damage[s] to tangible property are 'economic damage' in personal-injury cases, but they are not 'economic loss' for purposes of the" *Liability for Economic Harm* volume of the *Restatement (Third) of Torts* series), but physical injury to tangible property is likewise never an alleged injury in a cyberattack class action.

valuation.[12] Pain and suffering, inconvenience, emotional distress, loss of society and companionship, loss of enjoyment of life ("hedonic" damages), injury to reputation, and humiliation are all examples of intangible non-economic injuries.[13] In the cyberattack context, injuries of this sort include those described in Items (1), (2), (6), and (10) of the *UnitedHealth* injury allegations and also, where they are not alleged to have caused the plaintiff a lost economic opportunity measurable by reference to a market valuation, those described in Items (7) and (8) and the non-expense component of Item (9) of those allegations.

Cyberattack class action complaints typically assert a wide range of differing theories seeking to hold the entity that suffered the cyberattack in question liable for the named plaintiff's and the putative class members' alleged injuries by reason of the attack.[14] From the inception of this species of class action, cyberattack class actions have asserted common-law negligence as one such theory of liability, asserting that the entity suffering the cyberattack at issue did not have in place reasonable security measures to protect the personal information in question against the attack that occurred.[15] That approach continues unabated today, as modern cyberattack class action complaints

12. *See* Apportionment of Liability Restatement, *supra* note 7, § E18 (defining "non-economic damages") and Remedies Restatement, *supra* note 11, § 20, comment d (elaborating on distinction between economic and non-economic damages).

13. *See* Apportionment of Liability Restatement, *supra* note 7, § E18, comment c (listing examples of "non-economic damages").

14. *See, e.g.*, UnitedHealth Complaint, *supra* note 2, at Counts I-XLI (asserting 41 separate theories of liability).

15. *See* Amended Complaint (Docket No. 19), Sovereign Bank v. BJ's Wholesale Club, Case No. 1:05-cv-1150 (M.D. Pa., filed Nov. 7, 2005), at Count I ("Negligence"), ¶¶ 36-43.

regularly include a negligence claim as their very first cause of action.[16]

Plaintiffs bringing such negligence claims craft their pleadings so as to try to allege the traditional elements of a common-law negligence claim: (1) duty; (2) breach of duty; (3) injury; (4) but-for causation of injury; and (5) reasonable foreseeability of injury.[17] In so doing, cyberattack class action plaintiffs typically assert that each injury asserted in their complaint—whether of the economic or non-economic variety, as defined above—is an injury sufficient to satisfy the injury element of the common-law negligence claim that normally leads off the complaint's list of causes of action.[18] For their part, cyberattack class action defendants frequently defend against the complaint's negligence claim by asserting that some or all of the complaint's alleged injuries, even if proven, would not sustain a claim in common-law

16. Based on this author's review and count, during the period from Jan. 1, 2025 through June 30, 2025, Law360's *Privacy & Cybersecurity* newsletter reported on 62 cyberattack class action complaints that had been filed in the U.S. courts (not counting a few such complaints that were filed against federal or state governmental entities that would have had a sovereign immunity defense to a common-law negligence claim). Every single one of those 62 complaints asserted a common-law negligence claim, and, in all but two of those 62 complaints, the negligence claim was asserted as the complaint's very first count.

17. *See* Cornell Law School, Legal Information Institute, "Negligence" (specifying the five elements of a claim in common-law negligence), available at www.law.cornell.edu/wex/negligence; *see, e.g.*, UnitedHealth Complaint, *supra* note 2, at Count I ("Negligence"), alleging duty (¶¶ 401-08), breach of duty (¶ 409), injury (¶¶ 413-14), but-for causation of injury (¶¶ 411-12), and reasonable foreseeability of injury (¶¶ 411-12).

18. *See, e.g.*, UnitedHealth Complaint, *supra* note 2, at Count I ("Negligence"), ¶ 413 (asserting that each of the ten items of injury alleged in Paragraph 15 of the complaint, *see supra* note 6 and accompanying text, is sufficient to sustain the complaint's negligence count).

negligence. Unsurprisingly then, many U.S. courts have been called upon to decide whether an "injury" alleged in the complaint in a cyberattack class action is an "injury" actionable in common-law negligence. Unfortunately, as shown below, the U.S. courts have thus far been unsuccessful in answering this question coherently, as they have employed differing analytical frameworks, and arrived at disparate conclusions, regarding what sorts of cyberattack-caused injuries are actionable in negligence.

A. Economic Injuries

The types of injuries alleged by plaintiffs in cyberattack class actions typically include some or all of such items as (1) out-of-pocket costs of fraud and other identity theft perpetrated by means of personal information stolen in the cyberattack[19]; (2) expenses of measures taken to prevent such fraud and other identity theft from occurring[20]; (3) diminution, by reason of the theft and consequent availability of the personal information in question, in the market value of that information[21]; and (4) lost "benefit of the bargain" by reason of the failure of the entity that suffered the cyberattack to provide the promised or otherwise legally required security for the personal information involved in the cyberattack, on the theory that such failure caused the plaintiff either to overpay for a product or service he or she purchased from that entity or to be under-compensated for employment services he or she rendered to that entity.[22] All of these

19. *See, e.g.*, UnitedHealth Complaint, *supra* note 2, ¶ 15, Item (3).

20. *See, e.g.*, *Id* ¶ 15, Item (9).

21. *See, e.g.*, *Id* ¶ 15, Items (4) and (5).

22. *See, e.g.*, CPS Solutions Complaint, *supra* note 9, at ¶ 108 (alleging lost benefit of the bargain on an overpayment-for-services theory of this sort);

alleged injuries are "economic injuries" within the meaning of this article, as they all are pecuniary injuries with respect to which a market exists (or allegedly exists) and that therefore can be valued by reference to the market's valuation of the injury.[23] The complaints in cyberattack class actions typically assert that each of these economic injuries is sufficient to sustain the complaint's common-law negligence claim.[24] As a result, a number of U.S. courts have been called upon to decide whether economic injuries of this sort are actionable in common-law negligence and therefore capable of sustaining the negligence claim that appears in virtually every cyberattack class action complaint. As shown below, to date the U.S. courts have offered wildly divergent answers to that question.

For the most part, the debate within the U.S. courts as to whether the economic injuries typically alleged in a cyberattack class action are actionable in common-law negligence has turned on those courts' understanding and application of the so-called "economic-loss rule." Traditionally, "the law g[ave] protection against negligent acts to the security of the person, and all interests in personal property," such that "negligence m[ight]

OBI Seafoods Complaint, *supra* note 10, at ¶ 120 (alleging lost benefit of the bargain on an under-compensation theory of this sort).

23. *See supra* notes 7-8 and accompanying text.

24. *See, e.g.*, UnitedHealth Complaint, *supra* note 2, at Count I ("Negligence"), ¶ 413 (asserting that each of the economic injuries alleged in Paragraph 15 of the complaint, *see supra* note 6 and accompanying text, is sufficient to sustain the complaint's negligence count); CPS Solutions Complaint, *supra* note 9, at Count I ("Negligence"), ¶ 153(v) (asserting that plaintiff's alleged lost benefit of the bargain on the overpayment-for-services theory is an injury sufficient to sustain the complaint's negligence count); OBI Seafoods Complaint, *supra* note 10, at Count I ("Negligence"), ¶ 153(iv) (asserting that plaintiff's alleged lost benefit of the bargain on the under-compensation theory is an injury sufficient to sustain the complaint's negligence count).

result in liability [only] for personal injury or property damage."[25] The "economic-loss rule" traditionally acted (and where and when it is applicable still acts today) as a corollary to that principle, by providing that "there is generally no liability in [negligence] for causing pure economic loss to another."[26] As the economic injuries typically alleged in a cyberattack class action are always "pure economic loss," in that injuries of that sort always represent alleged "financial loss[es] not arising from injury to the plaintiff's person or from physical harm to the plaintiff's property,"[27] those injuries are as a matter of law not actionable in common-law negligence where, and when, the economic-loss rule applies.[28]

---

25. William L. Prosser, *Handbook of the Law of Torts* § 54 , WEST PUBLISHING CO., (4th ed. 1971) (hereinafter "Prosser").

26. *See* Restatement (Third) of Torts: Liability for Economic Harm (Am. L. Inst. 2020) (hereinafter "Economic Harm Restatement"), § 1, comment a (setting forth traditional formulation of the economic-loss rule).

27. *See id*. § 1, comment a, and § 2 (defining "economic loss").

28. Some U.S. courts have held that the economic-loss rule, when applicable, prohibits negligence claims from being based on *any* injury other than physical harm to person or property and thus makes both economic injuries and non-economic injuries (as those terms are defined in this article, *see supra* notes 7-10 and 11-13 and accompanying text) allegedly caused by a cyberattack inactionable in common-law negligence. *See, e.g.*, Mohsen v. Veridian Credit Union, 733 F. Supp. 3d 754, 767 (N.D. Iowa 2024) (Iowa economic-loss rule bars negligence claim based on emotional distress allegedly caused by a cyberattack); Bellwether Cmty. Credit Union v. Chipotle Mexican Grill, Inc., 353 F. Supp. 3d 1070, 1083 (D. Colo. 2018) ("Bellwether") ("Economic loss [for purposes of the economic loss rule] is defined generally as damages other than physical harm to persons or property."). Decisions of this sort therefore refuse to find cyberattack-caused non-economic injuries actionable in common-law negligence for reasons that are separate and apart from the reasons set forth in the cases discussed *infra* in Part I.B.1. Those cases thus further contribute to the decisional quagmire described *infra* in Parts I.B.1 and I.B.2.

Many U.S. courts have invoked the economic-loss rule in holding that the economic injuries typically alleged in a cyberattack class action are not actionable in common-law negligence.[29]

---

29. *See, e.g.*, Terpin v. AT&T Mobility LLC, 118 F.4th 1102, 1114-16 (9th Cir. 2024) ("Terpin") (California economic loss rules precludes recovery in negligence of purely economic losses caused by a cyberattack); Community Bank of Trenton v. Schnuck Markets Inc., 887 F.3d 803, 818-18 (7th Cir. 2018) (Illinois and Missouri economic loss rules preclude recovery in negligence of purely economic losses caused by a cyberattack); Silverpop Systems Inc. v. Leading Market Technologies, Inc., 641 F. App'x 849, 852-54 (11th Cir. 2016) (per curiam), aff'g in relevant part, No. 12-cv-2513-SCJ, 2014 WL 11164763 (N.D. Ga. Feb. 18, 2014) (Georgia economic loss rule precludes recovery of purely economic losses caused by a cyberattack); In re TJX Companies Retail Sec. Breach Litig., 564 F.3d 489, 498 (1st Cir. 2009), as amended on reh'g in part (May 5, 2009) (upholding dismissal of negligence claim in a cyberattack class action because, under Massachusetts law, "purely economic losses are unrecoverable in tort and strict liability actions [based on a cyberattack] in the absence of personal injury or property damage"); Morales v. Conifer Revenue Cycle Solutions, LLC, 2025 U.S. Dist. LEXIS 65180, at *17-18 (C.D. Cal. Mar. 31, 2025) ("Morales") (California economic loss rule precludes recovery of purely economic losses caused by a cyberattack); Jones v. Sturm, Ruger & Co., 2024 U.S. Dist. LEXIS 54804, at *16-19 (D. Conn. Mar. 27, 2024) (Connecticut economic loss rule precludes recovery of purely economic losses caused by a cyberattack); Salas v. Acuity-CHS, LLC, 2023 U.S. Dist. LEXIS 54825, at *19-20 (D. Del. Mar. 30, 2023) ("Salas") (Delaware economic loss rule precludes recovery of purely economic losses caused by a cyberattack); Brickman v. Maximus, Inc., 2023 U.S. Dist. LEXIS 46038, at *5-9 (S.D. Ohio Mar. 17, 2023) (Ohio economic loss rule precludes recovery of purely economic losses caused by a cyberattack); Aspen Am. Ins. Co. v. Blackbaud, Inc., 625 F. Supp. 3d 982, 1001-1005 (N.D. Ind. 2022) ("Blackbaud II") (Indiana economic loss rule precludes recovery of purely economic losses caused by a cyberattack); Bellwether, *supra* note 28, 353 F. Supp. 3d at 1083-85 (Colorado economic loss rule precludes recovery of purely economic losses caused by a cyberattack); In re Capital One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 401 (E.D. Va. 2020) ("Capital One") (Washington economic loss rule precludes recovery of purely economic losses caused by a cyberattack); Hameed-Bolden v. Forever 21 Retail, Inc., 2018 U.S. Dist. LEXIS 217868, at

Many other U.S. courts, on essentially identical facts, have declined to so invoke the economic-loss rule. Those courts cite a wide range of rationales for so declining:

---

*12-19 (C.D. Cal. Oct. 1, 2018) (California economic loss rule precludes recovery of purely economic losses caused by a cyberattack); In re SuperValu, Inc., Customer Data Sec. Breach Litig., 2018 U.S. Dist. LEXIS 36944, *36-38 (D. Minn. Mar. 7, 2018) ("SuperValu") (Illinois economic loss rule precludes recovery of purely economic losses caused by a cyberattack), *aff'd sub. nom* Alleruzzo v. SuperValu, Inc., 925 F.3d 955 (8th Cir. 2019); In re Target Corp. Customer Data Security Breach Litigation, 66 F. Supp. 3d 1154, 1171-76 (D. Minn. 2014) ("Target Customer Litigation") (dismissing, under the Massachusetts, California, Illinois, Iowa, and Alaska economic loss rules, negligence claim seeking to recover economic losses allegedly caused by a cyberattack that resulted in theft of plaintiffs' personal information); In re Sony Gaming Networks & Customer Data Security Breach Litigation, 996 F. Supp. 2d 942, 966-73 (S.D. Cal. 2014) (dismissing, under the Massachusetts and California economic loss rules, negligence claim seeking to recover economic losses allegedly caused by a cyberattack that resulted in theft of plaintiffs' personal information); In re Heartland Payment Systems, Inc. Customer Data Security Breach Litigation, 834 F. Supp. 2d 566, 590 (S.D. Tex. 2011), *rev'd sub. nom in part on other grounds*, Lone Star Nat'l Bank v. Heartland Payment Sys., 729 F.3d 421 (5th Cir. 2013) (dismissing, under the Texas economic-loss rule, negligence claim seeking to recover economic losses allegedly caused by a cyberattack that resulted in theft of personal information in plaintiffs' custody); In re Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 528-31 (N.D. Ill. 2011) (Illinois economic loss rule precludes recovery in negligence of purely economic losses caused by a cyberattack); Sovereign Bank v. BJ's Wholesale Club, Inc., 395 F. Supp. 2d 183, 204 (M.D. Pa. 2005), *aff'd in relevant part*, 533 F.3d 162, 175-78 (3d Cir. 2008) (dismissing, under the Pennsylvania economic loss rule, negligence claim seeking to recover economic losses allegedly caused by a cyberattack that resulted in theft of personal information in defendant's custody); Cumis Insurance Society, Inc. v. BJ's Wholesale Club, Inc., 918 N.E.2d 36, 46-47 (Mass. 2009) (upholding dismissal, under the Massachusetts economic loss rule, of negligence claim seeking to recover economic losses allegedly caused by a cyberattack that resulted in theft of personal information in defendant's custody).

- Some U.S. courts have found the economic-loss rule to be applicable only where, unlike the case before the court, a contract existed between the plaintiff and the defendant.[30]
- Others have found the rule to be inapplicable, even where the parties were in privity, where the negligence claim is founded not on an alleged breach of a duty created by the contract, but rather on an alleged breach of an independent common-law duty.[31]

---

30. *See, e.g.*, Wittmeyer v. Heartland All. for Hum. Needs & Rights, 2024 U.S. Dist. LEXIS 8803, at *8 (N.D. Ill. Jan. 17, 2024) ("Wittmeyer") (Illinois economic loss rule does not apply to cyberattack-based negligence claim where "the plaintiffs do not allege an express contract between the parties that would establish a duty by [defendant] to safeguard the plaintiffs' personal information"); Gordon v. Chipotle Mexican Grill, Inc., 2018 U.S. Dist. LEXIS 129928, *34-35 (D. Colo. Aug. 1, 2018) (Arizona economic loss rule does not apply to cyberattack-based negligence claim where parties are not in privity), *report aff'd and rev'd in part, on other grounds*, 344 F. Supp. 3d 1231 (D. Colo. 2018).

31. *See, e.g.*, Zimmerman v. Highmark, Inc., 2025 U.S. Dist. LEXIS 79813, at *17-19 (W.D. Pa. Apr. 28, 2025) ("Highmark") (economic-loss rule inapplicable to economic injuries allegedly caused by a cyberattack because defendant "had a common-law duty to protect [plaintiffs'] information"); Capital One, *supra* note 29, 488 F. Supp. 3d at 396-97, 397-401 (Texas and Virginia economic-loss rules inapplicable to negligence claims based on a cyberattack by reason of those states' "independent duty exception" to the rule); In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1321 (N.D. Ga. 2019) ("Equifax") (following *Home Depot*, cited below); In re Arby's Rest. Group Litig., 2018 U.S. Dist. LEXIS 131140, at *40-50 (N.D. Ga. Mar. 5, 2018) ("Arby's") (following *Home Depot*, cited below); In re Home Depot Inc., 2016 U.S. Dist. LEXIS 65111, at *28-29 (N.D. Ga. 2016) ("Home Depot") (Georgia economic-loss rule does not bar negligence claim based on purely economic losses caused by a cyberattack because defendant owed plaintiff an "independent duty" in common-law negligence to protect plaintiff's information against the attack); Target Customer Litigation, *supra* note 29, 66 F. Supp. 3d at 1171-76 (Georgia, New Hampshire, and New York economic-loss

- Other U.S. courts have found the economic-loss rule inapplicable in the cyberattack class action context, even where the parties are in privity, on the ground that the rule only applies in products liability cases and/or has no application to service contracts.[32]

---

rules do not bar negligence claim based on purely economic losses caused by a cyberattack because defendant owed plaintiff an "independent duty" to protect plaintiff's information against the attack); Flores v. Aon Corp., 242 N.E.3d 340, 360-61 (Ill. App. 5th Dist. 2023) (declining to apply Illinois economic-loss rule in a cyberattack case, where injury arose from alleged breach of common law duty to safeguard personal information and not from an alleged breach of duty imposed by a contract between the parties); Dittman v. UPMC, 649 Pa. 496, 499, 196 A.3d 1036, 1054 (2018) (under Pennsylvania's economic loss doctrine, recovery for purely pecuniary damages caused by a cyberattack is permissible under a negligence theory provided that the plaintiff can establish the defendant's breach of a legal duty arising under common law that is independent of any duty assumed pursuant to contract). As pointed out by a leading commentary on the U.S. courts' application of the economic-loss rule to negligence claims arising out of cyberattacks, where (as in the *Equifax*, *Arby's*, and *Home Depot* decisions cited above, among others) the "independent duty" is a duty owed in common-law negligence, the independent duty "exception" entirely swallows the economic-loss rule. *See* Catherine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DePaul L. Rev. 339, 377 (2017) ("The court's analysis [in *Home Depot*] shows how the ['independent duty'] exception can swallow the rule. . . .").

32. *See, e.g.*, Priddy v. Zoll Med. Corp., 2025 U.S. Dist. LEXIS 62112, at *35 (D. Mass. Mar. 31, 2025) ("Priddy") (cyberattack class action case holding that Florida's economic-loss rule applies only in product liability cases and thus had no application to plaintiff's cyberattack-based negligence claim); Brooks v. Peoples Bank, 732 F.Supp.3d 765, 778-79 (S.D. Ohio 2024) (Kentucky economic-loss rule applies only to product liability claims and thus has no application to negligence claim asserted in a cyberattack class action); Toretto v. Donnelley Financial Solutions, Inc., 583 F.Supp.3d 570, 590 (S.D.N.Y. 2022) ("Donnelly") (cyberattack case declining to apply New York's economic loss rule outside the context of products liability); In re Mednax Services, Inc., Customer Data Security Breach Litigation, 603 F.Supp.3d 1183, 1224 (S.D. Fla. 2022) (same holding as *Priddy*, cited earlier in this footnote); Capital One,

- Other U.S. courts have found the economic-loss rule inapplicable to the economic injuries typically alleged in a cyberattack class action where, as in the case before the court, the parties allegedly had either a fiduciary[33] or a "special"[34] relationship.

---

supra note 29, 488 F. Supp. 3d at 395-96 (same holding as *Priddy*, cited earlier in this footnote); Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 749 (S.D.N.Y. 2017) (cyberattack case declining to apply New York's economic loss rule outside the context of products liability); Thawar v. 7-Eleven, Inc., 165 F. Supp. 3d 524, 532 (N.D. Tex. 2016) (cyberattack case declining to apply Texas's economic loss rule outside the context of products liability where parties were not in privity); Reetz v. Advocate Aurora Health, Inc., 405 Wis. 2d 298, 315-17, 983 N.W.2d 669, 678-79 (Wis. App. 2022) (cyberattack case declining to apply Wisconsin's economic loss rule where parties' contract was one for services and, accordingly, plaintiff's "claims of economic loss do not derive from a loss in value of any product or a loss attributable to a product defect").

33. *See, e.g.*, Doe v. Tenet Healthcare Corp., 731 F. Supp. 3d 142, 148 (D. Mass. 2024) (purely economic losses caused by a cyberattack actionable in negligence, notwithstanding the Massachusetts economic-loss rule, where defendant had a fiduciary relationship with the plaintiff); In re Shields Health Care Grp., Inc. Data Breach Litig., 721 F. Supp. 3d 152, 160-61 (D. Mass. 2024) ("Shields") (data breach claim sounding in negligence against provider of medical services allowed to go forward based on purely economic losses where the provider owed the plaintiff a fiduciary duty).

34. *See, e.g.*, Capital One, *supra* note 29, 488 F. Supp. 3d at 394-95 (California economic-loss rule does not bar negligence claim based on purely economic losses caused by a cyberattack because of alleged "special relationship" between defendant and plaintiff); *In re* Yahoo! Inc. Customer Data Sec. Breach Litig., 313 F. Supp. 3d 1113, 1131-33 (N.D. Cal. 2018) (same holding as *Capital One*, cited earlier in this footnote); Target Customer Litigation, *supra* note 29, 66 F. Supp. 3d at 1171-76 (District of Columbia, Idaho, and Pennsylvania economic-loss rules do not bar negligence claim based on purely economic losses caused by a cyberattack because of alleged "special relationship" between defendant and plaintiff).

- One seemingly outlier U.S. court has found the economic-loss rule inapplicable to the economic injuries typically alleged in a cyberattack class action where, as in the case before the court, "the defendant['s negligence] causes an identifiable class of plaintiffs to which it owes a duty of care to suffer economic loss that does not result in boundless liability."[35]

The net result is a mishmash of rulings in which the U.S. courts have reached differing outcomes on identical facts based on differing judges' different understandings of the economic-loss rule.

Moreover, the decisional mishmash does not end with the U.S. courts' application or non-application of the economic-loss rule to the economic injuries typically alleged in a cyberattack class action. For example, U.S. courts have come to differing conclusions as to whether a cyberattack class action plaintiff can sue in negligence to recover the out-of-pocket expenses that such a plaintiff typically claims to have incurred[36] to mitigate the risk of him or her suffering identity theft or other fraud at some

35. Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc., 729 F.3d 421, 424 (5th Cir. 2013) (applying New Jersey law). As it is difficult to imagine a cyberattack class action where the class affected by the defendant's allegedly negligent conduct is not "identifiable" or the defendant's liability to that class would be "boundless," as a practical matter under this reading of New Jersey law the economic-loss rule never would have any applicability in a cyberattack class action.

36. *See, e.g.*, UnitedHealth Complaint, *supra* note 2, ¶ 15, Item (9) (alleging that the named plaintiffs incurred expenses of this sort) and at Count I ("Negligence"), ¶ 413 (asserting that the expenses alleged in Item (9) of Paragraph 15 of the complaint are sufficient to sustain the complaint's negligence count).

point in the future by reason of the cyberattack in question.[37] Similarly, U.S. courts have ruled differently from one another as

37. *Compare, e.g.*, Roma v. Prospect Med. Holdings, Inc., 2024 U.S. Dist. LEXIS 138947, at *26-27 (E.D. Pa. Aug. 5, 2024) ("financial costs incurred mitigating the materialized risk and imminent threat of identity theft" from a data breach are actionable in negligence); Shields, *supra* note 33, 721 F. Supp. 3d at 161 ("Where Plaintiffs show a substantial risk of harm manifesting in the future, the 'element of injury and damage will have been satisfied and the cost of that monitoring is recoverable in tort.'"); Smallman v. MGM Resorts International, 638 F.Supp.3d 1175, 1192-93 (D. Nev. 2022) ("MGM Resorts") (out-of-pocket costs for identity theft protection services recoverable in negligence where reasonably incurred in response to a cyberattack); Everhart v. Colonial Pipeline Co., 2022 U.S. Dist. LEXIS 155295, at *11-14 (N.D. Ga. July 22, 2022) ("Colonial Pipeline") (costs of monitoring to mitigate risk of future identity theft by reason of a cyberattack recoverable where harm is shown to be both substantial and imminent); Donnelley, *supra* note 32, 583 F.Supp.3d at 590 ("Because Plaintiffs face a substantial risk of identity theft or fraud, Plaintiffs' costs incurred to mitigate that threat satisfy the damages element of their [negligence] claim."); In re Blackbaud, Inc, 567 F. Supp. 3d 667, 686-87 (D.S.C. 2021) ("Blackbaud I") (money spent "to mitigate [plaintiffs'] exposure to identity theft or fraud as a result of the [cyberattack]" is actionable in common-law negligence under South Carolina law); In re Marriott Int'l, Inc., 440 F. Supp. 3d 447, 494-95 (D. Md. 2020) ("Marriott") (money spent to mitigate potential harm from a cyberattack actionable in negligence under Maryland and Florida law where potential harm is not speculative) *with, e.g.*, Pisciotta v. Old National Bancorp, 499 F.3d 629, 639 (7th Cir. 2007) ("Pisciotta ") ("[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy" by expending time and resources to monitor and protect their identities"); Gannon v. Truly Nolen of Am. Inc., 2023 U.S. Dist. LEXIS 181410, at *5-7 (D. Ariz. Aug. 31, 2023) ("Gannon") (negligence claim may not be predicated on out-of-pocket expenses allegedly incurred to reduce risk of future injury by reason of a cyberattack absent sufficient allegations that such expenses were reasonable and necessary); Blackbaud II, *supra* note 29, 625 F. Supp. 3d at 998 ("cost of credit monitoring to mitigate a risk of future identity theft is not a compensable injury in Indiana"); Attias v. CareFirst, Inc., 365 F. Supp. 3d 1, 13-16 (D.D.C. 2019) ("Attias I") (cost of prophylactic measures to

to whether a cyberattack class action plaintiff can sue in negligence to recover the amount by which the market value of his or her personal information was diminished by reason of that personal information becoming otherwise available to the market by means of the cyberattack in question[38] or the amount by

---

prevent future identity theft not actionable in negligence where no actual injury, such as misuse of the stolen data, has been alleged); Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 783 (W.D. Mich. 2006) (rejecting, under Michigan law, "plaintiff's position that the purchase of credit monitoring constitutes either actual damages or a cognizable loss . . . based on a risk of injury at some indefinite time in the future"); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1020-21 (D. Minn. 2006) (rejecting, under Minnesota law, plaintiffs' contention for both negligence and breach-of-contract claims "that the time and money they have spent monitoring their credit suffices to establish damages" in "anticipation of future injury that has not materialized").

38. *Compare, e.g.,* In re Accellion, Inc. Data Breach Litig., 2024 U.S. Dist. LEXIS 15525, at *30-31 (N.D. Cal. Jan. 29, 2024) ("Accellion") (loss of value of personal information by reason of a cyberattack viable theory of injury for purposes of a negligence claim under California law); Blackbaud I, *supra* note 37, 567 F. Supp. 3d at 686-87 ("loss of value in [plaintiffs'] Private Information" by reason of a cyberattack is an injury actionable in negligence under South Carolina law); MGM Resorts, *supra* note 37, 638 F.Supp.3d at 1190-91 (following holding in *Marriott*, cited below); Marriott, *supra* note 37, 440 F. Supp. 3d at 494-95 (lost value of personal information by reason of a cyberattack is an injury actionable in negligence under Maryland and Florida law) *with, e.g.,* Feathers v. On Q Financial LLC, 2025 U.S. Dist. LEXIS 121338, at *35-36 (D. Ariz. June 25, 2025) ("Feathers") (same holding as *Yuma Regional*, cited later in this footnote); Morales, *supra* note 29, 2025 U.S. Dist. LEXIS 65180, at *15-16 (same holding as *Yuma Regional*, cited later in this footnote); Johnson v. Yuma Reg'l Med. Ctr., 2024 U.S. Dist. LEXIS 207602, at *11-14 (D. Ariz. Nov. 14, 2024) ("Yuma Regional") (plaintiffs' allegations of a diminution in the value of their personal information by reason of a cyberattack insufficient to sustain a negligence claim); Landon v. TSC Acquisition Corp., 2024 U.S. Dist. LEXIS 237108, at *15-16 (C.D. Cal. Nov. 1, 2024) ("TSC Acquisition") (same holding as *Yuma Regional*, cited earlier in this footnote); Gannon, *supra* note 37, 2023 U.S. Dist. LEXIS 181410, at *5-7 (negligence claim

which he or she allegedly overpaid for the defendant's product or service, or was underpaid for his or her services as an employee, by reason of the defendant's alleged failure to provide the promised or otherwise legally required security for his or her personal information.[39]

---

may not be predicated on alleged lost value of personal information by reason of a cyberattack); Wittmeyer, *supra* note 30, 2024 U.S. Dist. LEXIS 8803, at *8 ("Illinois has decline[d] to hold that the alleged diminution in value of plaintiffs' personal information [by reason of a cyberattack] amounts to actual monetary damages.") (internal quotation omitted); In re USAA Data Security Litigation, 621 F.Supp.3d 454, 470-71 (2022) ("USAA") ("Plaintiffs thus do not plausibly allege damages based on the lost value of their driver's license numbers."); Rand v. Travelers Indem. Co., 637 F. Supp. 3d 55, 70-71 (S.D.N.Y. 2022) ("Travelers") (alleged lost value of personal information by reason of a cyberattack cannot sustain a negligence claim under New York law where plaintiff "does not plausibly allege damages based on her PII's lost value"); Colonial Pipeline, *supra* note 37, 2022 U.S. Dist. LEXIS 155295, at *6-8 (alleged diminution in market value of plaintiff's personal information by reason of a cyberattack too speculative of an injury to sustain a negligence claim under Georgia law); Capital One, *supra* note 29, 488 F. Supp. 3d at 403-04 (where complaint "failed to plausibly allege damages based on the lost or reduced value of [plaintiffs'] PII" by reason of a cyberattack, such alleged lost value could not sustain a negligence claim).

39. *Compare, e.g.*, Yuma Regional, *supra* note 38, 2024 U.S. Dist. LEXIS 207602, at *14-15; Capital One, *supra* note 29, 488 F. Supp. 3d at 404-05, and Attias I, *supra* note 37, 365 F. Supp. at 12-13 (all holding alleged overpayment for defendant's services not sufficiently plausible to sustain cyberattack class action complaint's negligence and other claims) *with, e.g.*, TSC Acquisition, *supra* note 38, 2024 U.S. Dist. LEXIS 237108, at *17-18 (following *MGM Resorts*, cited below in this footnote); MGM Resorts, *supra* note 37, 638 F.Supp.3d at 1189-90 (alleged overpayment for defendant's services is an injury sufficient to sustain a cyberattack class action complaint's negligence claim under California law); Marriott, *supra* note 37, 440 F. Supp. 3d at 494-95 (alleged overpayment for defendant's services is an injury sufficient to sustain a cyberattack class action complaint's negligence claim under Maryland and Florida law).

In short, the U.S. courts' rulings to date have created a jurisprudential quagmire on the question of whether the economic injuries typically alleged in a cyberattack class action are actionable in common-law negligence.

B. Non-Economic Injuries

In cyberattack class actions, the injuries allegedly suffered by the individuals whose personal information was involved in the cyberattack in question typically include (1) loss of privacy;[40] (2) misappropriation of their identity, name and likeness;[41] (3) emotional and mental distress and anguish resulting from the access, theft and/or posting of their personal information;[42] (4) disruption of their lives;[43] (5) time and effort expended responding to and preventing the threats and harm posed by the cyberattack,[44] and (6) a continued substantial and imminent risk of the misuse of their personal information.[45] All of these alleged injuries are "non-economic injuries" within the meaning of this article, as they all are injuries with respect to which no market exists and that therefore cannot be valued by reference to a market valuation, putting them outside the scope of this article's

40. *See, e.g.*, UnitedHealth Complaint, *supra* note 2, ¶ 15, Item (1).

41. *See, e.g., Id*, ¶ 15, Item (2)

42. *See, e.g., Id*, ¶ 15, Item (6)

43. *See, e.g., Id*, ¶ 15, Items (7) and (8)

44. *See, e.g., Id*, ¶ 15, Item (9). As noted above, this particular item would be a non-economic injury only where it is not alleged to have had an associated opportunity cost measurable by reference to some market, such as foregone earnings; otherwise, it would be an economic injury within the scope of the discussion presented in Part II.A of this Article. *See supra* notes 7-13 and accompanying text.

45. *See, e.g., Id*, ¶ 15, Item (10).

definition of "economic injuries."[46] The complaints in cyberattack class actions typically assert that each of these non-economic injuries is sufficient to satisfy the "injury" element of the complaint's common-law negligence claim.[47] As a result, a number of U.S. courts have been called upon to decide whether non-economic injuries of this sort are actionable in common-law negligence and therefore capable of sustaining the negligence claim that appears in virtually every cyberattack class action complaint.[48] As shown below in this Part I.B, to date the U.S. courts have offered wildly divergent answers to that question,[49] just as

---

46. *See supra* notes 10-13 and accompanying text.

47. *See, e.g.*, UnitedHealth Complaint, *supra* note 2, at Count I ("Negligence"), ¶ 413 (asserting that each of the non-economic injuries alleged in Paragraph 15 of the complaint, *see supra* note 6 and accompanying text, is sufficient to sustain the complaint's negligence count).

48. *See supra* note 18 and accompanying text.

49. Some courts upholding the actionability in negligence of non-economic injuries have either arrived at or sought to bolster their readings of the relevant state law by pointing to the fact that the injury in question is (in their view) "concrete" for purposes of deciding whether that injury can support the plaintiff's Article III standing in regard to his or her negligence claim. *See, e.g.*, Bohnak v. Marsh & McLennan Cos., 79 F.4th 276, 289-90 (2d Cir. 2023) (alleged injury can support a negligence claim where the injury is cognizable for Article III standing purposes); Highmark, *supra* note 31, 2025 U.S. Dist. LEXIS 79813, at *19 ("For the same reasons that Plaintiffs' injuries are concrete [for Article III standing purposes], they satisfy the injury element for a negligence claim"); Allen v. Wenco Mgmt., LLC, 696 F. Supp. 3d 432, 437-38 (N.D. Ohio 2023) ("Wenco") (finding plaintiff's "loss of privacy" by reason of a cyberattack to be an injury sufficient to sustain a negligence claim based on court's conclusion that such a loss of privacy is an injury sufficient to sustain Article III standing); Quora, *infra* note 53, 2019 U.S. Dist. LEXIS 235733, at *22 (supporting court's holding that cyberattack-caused loss of time and increased risk of identity theft are injuries actionable in negligence by cross-referencing court's earlier holding that they are injuries sufficient to sustain Article III standing). The reasoning of such courts is badly flawed, in this

they have (as discussed above in Part I.A) offered wildly divergent answers to the question of whether economic injuries of the sort typically alleged in cyberattack class actions are actionable in common-law negligence.

1. Impactful Non-Economic Injuries

Most of the non-economic injuries typically alleged in a cyberattack class action are injuries where the plaintiff(s) did or felt *something* by reason of the cyberattack in question, but that *something* cannot be valued by reference to a market and thus does not fall within this article's definition of an "economic

---

author's view. The Article III question (namely, whether the plaintiff has pled an injury sufficient to bring the negligence claim in federal court) is entirely different from, and thus cannot inform the answer to, the state-law issue (namely, whether the plaintiff has pled an injury sufficient to prevail on the negligence claim at trial), especially since "there is an even lower bar for the establishment of [Article III] standing than for pleading damages." Colonial Pipeline, *supra* note 37, 2022 U.S. Dist. LEXIS 155295, at *7 n.5 (citing Doe v. Chao, 540 U.S. 614, 625 (2004) (explaining that the plaintiff adequately showed injury sufficient for standing, but did not show damages)); *see* Alleruzzo v. SuperValu, Inc., 870 F.3d 763, 773 (8th Cir. 2017) ("Article III presents only a threshold inquiry," such that pleading deficiencies that do not defeat Article III standing as to a cyberattack-based negligence claim "could be fatal to the complaint under the higher hurdles of Rules 8(a) and 12(b)(6)") (internal quotations omitted); Krottner v. Starbucks Corp., 406 F. App'x 129, 131 (9th Cir. 2010) ("our holding that Plaintiffs-Appellants pled an injury-in-fact for purposes of Article III standing does not establish that they adequately pled damages for purposes of their state-law claims based on a cyberattack); Minka Lighting, *infra* note 54, 2023 U.S. Dist. LEXIS 81398, at *22 ("Although Plaintiff has sufficiently alleged an injury in fact for standing purposes, Plaintiff must still plead sufficient allegations to satisfy the damages requirement for his [cyberattack-based] negligence cause of action."); Attias I, *supra* note 37, 365 F. Supp. at 5 ("[W]hile plaintiffs' alleged [data breach] injuries may be enough to establish standing at the pleading stage of the case, they are largely insufficient to satisfy the 'actual damages' element of nine of their state-law causes of action.").

injury."[50] Examples of such "impactful" non-economic injuries are where the cyberattack allegedly caused the plaintiff(s) to suffer emotional distress, or to incur time and/or effort (but not a market-measurable opportunity cost) to address the cyberattack, or to have their lives disrupted in some other non-market-measurable fashion.[51]

To date, U.S. courts have not developed a consensus as to whether impactful non-economic injuries such as these are actionable in a negligence claim based on a cyberattack. Some courts have allowed negligence claims to go forward based on alleged emotional distress[52] or expenditure of time and/or effort

50. *See supra* note 7 and accompanying text (so defining "economic injury" for purposes of this article, based on the identical definition of "economic damages" set forth in the Apportionment of Liability Restatement).

51. *See, e.g.*, UnitedHealth Complaint, *supra* note 2, ¶ 15, Items (6)-(9).

52. *See, e.g.*, Castillo v. Berry Bros. Gen. Contrs. Inc., 2025 U.S. Dist. LEXIS 67295, at *11-12 (W.D. La. Apr. 8, 2025) ("Castillo") (emotional distress caused by a cyberattack actionable in negligence under Louisiana law); TSC Acquisition, *supra* note 38, 2024 U.S. Dist. LEXIS 237108, at *20 (emotional distress caused by a cyberattack actionable in negligence under California law); Baton v. Ledger SAS, 740 F. Supp. 3d 847, 911 (N.D. Cal. 2024) ("Baton") (emotional distress caused by a cyberattack actionable in negligence under California law); In re Arthur J. Gallagher Data Breach Litigation, 631 F.Supp.3d 573, 587 (N.D. Ill. 2022) ("emotional harms such as anxiety and increased concerns for the loss of privacy" are "types of non-economic damages [that] are recoverable under Illinois law"); Bowen v. Paxton Media Grp., LLC, 2022 U.S. Dist. LEXIS 162083, at *16-17 (W.D. Ky. Sept. 8, 2022) ("mental distress related to [plaintiffs'] fear of identity theft" and "stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach" actionable in negligence in a cyberattack case under Kentucky, Virginia, California, and Arkansas law); Mulkey v. Roundpoint Mortg. Servicing Corp., 2021 U.S. Dist. LEXIS 234110, at *9-10 (N.D. Ohio Dec. 6, 2021) ("Mulkey") (emotional distress caused by a cyberattack actionable in negligence under Ohio law); Ross v. AT&T Mobility, LLC, 2020 U.S. Dist. LEXIS 166298, at *39 n.9 (N.D.

or other life disruption[53] caused by a cyberattack. Others have refused to allow negligence claims in a cyberattack class action to go forward insofar as the injuries on which they are

Cal. May 14, 2020) (emotional distress caused by a cyberattack actionable in negligence under California law).

53. *See, e.g.*, Highmark, *supra* note 31, 2025 U.S. Dist. LEXIS 79813, at *19 ("spending time looking at credit card accounts, freezing accounts, [and] dealing with actual fraudulent activity," in response to a cyberattack, "is an injury actionable in negligence"); Baton, *supra* note 52, 740 F. Supp. 3d at 911 (negligence claim based on cyberattack may be based on "loss of time spent on credit monitoring, reviewing credit reports and fraud reports, implementing, and removing credit freezes, and contacting third parties to determine whether or not they had suffered fraud"); Gerber v. Twitter, Inc., 2024 U.S. Dist. LEXIS 58232, at *17-18 (N.D. Cal. Mar. 19, 2024) (time spent in addressing risk of identity theft from a cyberattack is actionable in common-law negligence under California law where pled as a privacy-based injury and the time's financial value is not being sought); Accellion, *supra* note 38, 2024 U.S. Dist. LEXIS 15525, at *30-31 (same); Kirsten v. California Pizza Kitchen, Inc., 2022 U.S. Dist. LEXIS 206552, at *17-19 (C.D. Cal. July 29, 2022) ("California Pizza Kitchen") (negligence claim in cyberattack class action may be predicated on "sharp increases in spam texts and calls since the breach"); Mulkey, *supra* note 52, 2021 U.S. Dist. LEXIS 234110, at *9-10 (lost time caused by a cyberattack actionable in negligence under Ohio law); In re GE/CBPS Data Breach Litig., 2021 U.S. Dist. LEXIS 146020, at *23-24 (S.D.N.Y. Aug. 4, 2021) ("GE/CBPS") ("time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; [and] time spent initiating fraud alerts" by reason of a cyberattack are all actionable injuries in negligence); Blackbaud I, *supra* note 37, 567 F. Supp. 3d at 686-87 (time spent in addressing risk of identity theft from a cyberattack is an injury actionable in common-law negligence under South Carolina law); Bass v. Facebook, Inc., 394 F. Supp. 3d 1024, 1039 (N.D. Cal. 2019) (time spent in addressing risk of identity theft from a cyberattack is an injury actionable in common-law negligence under California law where not pled as a purely economic loss); Hyunh v. Quora, Inc., 2019 U.S. Dist. LEXIS 235733, at *22 (N.D. Cal. Dec. 19, 2019) ("Quora") (loss of time by reason of a cyberattack is an injury sufficient to sustain a negligence claim).

predicated are merely emotional distress[54] or some other life inconvenience that did not cause an economic loss.[55] And still others have dismissed negligence claims based on such injuries on the ground that, while being "non-economic" within the

54. *See, e.g.*, Feathers, *supra* note 38, 2025 U.S. Dist. LEXIS 121338, at *36-37 (same holding as *Yuma Regional*, cited later in this footnote); Morales, *supra* note 29, 2025 U.S. Dist. LEXIS 65180, at *14-15 (same holding as *Yuma Regional*, cited later in this footnote); Yuma Regional, *supra* note 39, 2024 U.S. Dist. LEXIS 207602, at *17-18 (allegations of emotional distress by reason of a cyberattack, unaccompanied by allegations of any associated physical injury, insufficient to sustain a negligence claim); Salas, *supra* note 29, 2023 U.S. Dist. LEXIS 54825, at *19-20 (negligence claim may not be predicated on emotional distress caused by a cyberattack); Medoff v. Minka Lighting, LLC, 2023 U.S. Dist. LEXIS 81398, at *22-24 (C.D. Cal., May 8, 2023) ("Minka Lighting") (negligence claim may not be predicated on emotional distress caused by a cyberattack); Attias I, *supra* note 37, 365 F. Supp. 3d at 16 (dismissing negligence claim predicated on alleged cyberattack-induced emotional distress on the ground that such distress, unaccompanied by actual or threatened physical harm, is inactionable in negligence as a matter of law).

55. *See, e.g.*, Yuma Regional, *supra* note 38, 2024 U.S. Dist. LEXIS 207602, at *15-17, *18-19 (allegations of lost time spent dealing with or other inconvenience caused by a cyberattack, unaccompanied by allegations of any associated opportunity cost, insufficient to sustain a negligence claim); TSC Acquisition, *supra* note 38, 2024 U.S. Dist. LEXIS 237108, at *16-17 (same holding as *Yuma Regional*); Gannon, *supra* note 37, 2023 U.S. Dist. LEXIS 181410, at *5-7 (negligence claim may not be predicated on lost time caused by a cyberattack); Minka Lighting, *supra* note 54, 2023 U.S. Dist. LEXIS 81398, at *22-24 (negligence claim may not be predicated on inconvenience such as lost time caused by a cyberattack); MGM Resorts, *supra* note 37, 638 F.Supp.3d at 1192-93 (lost time in responding to a cyberattack not actionable in negligence); Travelers, *supra* note 38, 637 F. Supp. 3d at 70 ("the mere time and effort plaintiff allegedly expended addressing the consequences of the data breach, standing alone, are not cognizable" in negligence under New York law); USAA, *supra* note 38, 621 F.Supp.3d at 470 (same holding as *Travelers*, cited above in this footnote); SuperValu, *supra* note 29, 2018 U.S. Dist. LEXIS 36944, *34-35 (negligence claim may not be predicated on inconvenience such as lost time caused by a cyberattack).

meaning of this article, they nonetheless seek to recover "economic losses" within the meaning of, and thus are barred by, the relevant economic-loss rule.[56] Here, as with the U.S. courts' differing rulings as to the actionability in negligence of the economic injuries typically alleged in a cyberattack class action,[57] the courts' differing rulings arise not by reason of the facts differing from case to case, but rather from the courts' differing understandings of the injury element of a common-law negligence claim under the relevant state law.[58]

2. Non-Impactful Non-Economic Injuries

Some of the non-economic injuries typically alleged in a cyberattack class action are injuries that arise regardless of whether the plaintiff(s) did or felt something by reason of the cyberattack in question. Examples of "non-impactful" injuries of this sort are where the plaintiff claims to have been injured merely because the cyberattack resulted in the plaintiff's personal information being misappropriated, the privacy of that information being diminished, or the plaintiff's being put at risk of suffering some economic injury or impactful non-economic injury in the future.[59] Such injuries are "non-impactful" because they arise and exist whether or not the plaintiff was ever even aware of, much less did or felt something by reason of, the cyberattack in question.

---

56. See *supra* note 28.

57. See *supra* Part I.A.

58. *See* cases cited in notes 52-55 *supra* (all finding the injury in question to be as a matter of law either actionable, or non-actionable, under the state law the court viewed to be applicable to the negligence claim being asserted in the cyberattack class action in question).

59. *See, e.g.*, UnitedHealth Complaint, *supra* note 2, ¶ 15, Items (1), (2), and (10).

To date, as is the case with regard to *impactful* non-economic injuries, U.S. courts have likewise failed to develop a consensus as to whether *non-impactful* non-economic injuries such as these are actionable in a negligence claim based on a cyberattack. Some courts have allowed such negligence claims to go forward merely based on the cyberattack allegedly having put the plaintiff(s)' personal information into unauthorized hands[60] or its allegedly having put the plaintiff(s) at risk of suffering identity theft or some other economic injury at some future point in time.[61] Others have refused to allow such negligence claims to

60. *See, e.g.,* Bracy v. Americold Logistics LLC, 2025 U.S. Dist. LEXIS 28981, at *11 (N.D. Ga. Feb. 19, 2025) (under Georgia law, an injury actionable in negligence has been pled where "the allegations sufficiently assert that Plaintiffs' information is in the hands of criminals because of [a cyberattack]"); TSC Acquisition, *supra* note 38, 2024 U.S. Dist. LEXIS 237108, at *20 (plaintiff's "loss of privacy" by reason of a cyberattack is actionable injury in negligence under California law); Cahill v. Mem'l Heart Inst., LLC, 2024 U.S. Dist. LEXIS 174634, at *24-25 (E.D. Tenn. Sept. 26, 2024) ("Cahill") ("[p]rivacy harm" caused by theft of plaintiff's personal information in a cyberattack is actionable in negligence); Tracy v. Elekta, Inc., 667 F. Supp. 3d 1276, 1283 (N.D. Ga. 2023) ("an injury [actionable in negligence under Georgia law] exists where, at the very least, criminals have hacked into a data system and exfiltrated personally identifiable information and protected health information"); Wenco, *supra* note 49, 696 F. Supp. 3d at 437-38 (plaintiff's "loss of privacy" by reason of a cyberattack is an injury sufficient to sustain a negligence claim); Blackbaud I, *supra* note 37, 567 F. Supp. 3d at 686-87 ("unauthorized disclosure of [plaintiffs'] Private Information" by reason of a cyberattack is an injury actionable in negligence under South Carolina law); GE/CBPS, *supra* note 53, 2021 U.S. Dist. LEXIS 146020, at *23-24 ("loss of the confidentiality of the stolen confidential data" in a cyberattack is an injury actionable in negligence); Equifax, *supra* note 31, 362 F. Supp. 3d at 1315 (allegations that plaintiff's personal information was compromised in a cyberattack pleads a legally cognizable injury in negligence under common law).

61. *See, e.g.,* Cahill, *supra* note 60, 2024 U.S. Dist. LEXIS 174634, at *24-25 ("an increased risk of identity theft" caused by theft of plaintiff's personal information in a cyberattack is actionable in negligence); Briggs v. N.

go forward insofar as the injuries on which they are predicated are merely unauthorized data access[62] and/or future risk of

Highland Co., 2024 U.S. Dist. LEXIS 23538, at *22 (N.D. Ga. Feb. 9, 2024) (upholding negligence claim under Georgia law based on "Plaintiff's arguments and citation of authority on damages based on substantially increased risk of identity theft"); Shields, *supra* note 33, 721 F. Supp. 3d at 161 ("Where Plaintiffs show a substantial risk of harm manifesting in the future, the 'element of injury and damage will have been satisfied . . . ."); MGM Resorts, *supra* note 37, 638 F.Supp.3d at 1190-91 (increased risk of identity theft and fraud by reason of a cyberattack is an injury actionable in negligence); California Pizza Kitchen, *supra* note 53, 2022 U.S. Dist. LEXIS 206552, at *17-19 (increased risk of identity theft by reason of a cyberattack can sustain a negligence claim because it is "a 'privacy injury' that is not necessarily 'economic' in nature"); Blackbaud I, *supra* note 37, 567 F. Supp. 3d at 686-87 ("risk of extortion" and "risk of future identity theft or fraud" by reason of a cyberattack are injuries actionable in negligence under South Carolina law); GE/CBPS, *supra* note 53, 2021 U.S. Dist. LEXIS 146020, at *23-24 ("ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse" by reason of a cyberattack are injuries actionable in negligence); Equifax, *supra* note 31, 362 F. Supp. 3d at 1315 (allegations that plaintiffs' "all face a serious and imminent risk of fraud and identity theft due to the [cyberattack] . . . are sufficient to support a claim for relief" in common-law negligence under Georgia law); Collins v. Athens Orthopedic Clinic, 307 Ga. 555, 563-64, 837 S.E.2d 310, 316 (2019) (injury actionable in negligence under Georgia law has been pled where the plaintiff plausibly alleges "that the criminal theft of their personal data has left them at an imminent and substantial risk of identity theft").

62. *See, e.g.*, Minka Lighting, *supra* note 54, 2023 U.S. Dist. LEXIS 81398, at *22-24 & n.10 (negligence claim may not be predicated on "privacy injury" caused by misappropriation of plaintiff's personal information in a cyberattack); Colonial Pipeline, *supra* note 37, 2022 U.S. Dist. LEXIS 155295, at *8 ("the mere fact that a data breach occurred is not sufficient to show injury" for purposes of pleading a negligence claim); SuperValu, *supra* note 29, 2018 U.S. Dist. LEXIS 36944, *33-34 ("mere allegation of an unauthorized [use of data stolen in a cyberattack], unaccompanied by an out-of-pocket loss, is insufficient to state an actionable injury" in negligence).

identity theft.[63] And still others have dismissed negligence claims based on such injuries on the ground that, while being "non-economic" within the meaning of this article, they nonetheless seek to recover "economic losses" within the meaning of, and thus are barred by, the relevant economic-loss rule.[64] Here, as with the U.S. courts' differing rulings as to the actionability in negligence of the economic injuries and the impactful non-economic injuries typically alleged in a cyberattack class

63. *See, e.g.*, Pisciotta, *supra* note 37, 499 F.3d at 639 ("Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."); Feathers, *supra* note 38, 2025 U.S. Dist. LEXIS 121338, at *35 (same holding as *Yuma Regional*, cited later in this footnote); Castillo, *supra* note 52, 2025 U.S. Dist. LEXIS 67295, at *11 (same holding as *Yuma Regional*, cited later in this footnote); Yuma Regional, *supra* note 38, 2024 U.S. Dist. LEXIS 207602, at *19-20 (allegations of future risk of identity theft by reason of a cyberattack insufficient to sustain a negligence claim); TSC Acquisition, *supra* note 38, 2024 U.S. Dist. LEXIS 237108, at *19-20 (same holding as *Yuma Regional*); Gannon, *supra* note 37, 2023 U.S. Dist. LEXIS 181410, at *5-7 (negligence claim may not be predicated on risk of future injury by reason of a cyberattack);Travelers, *supra* note 38, 637 F. Supp. 3d at 70 (risk of future injury by reason of a cyberattack insufficient to sustain a negligence claim under New York law where plaintiff "does not plausibly allege she is 'reasonably certain' to incur expenses as a result of her greater exposure to the fraud"); USAA, *supra* note 38, 621 F. Supp. 3d at 470 (same holding as *Travelers*, cited above in this footnote); Attias I, *supra* note 37, 365 F. Supp. 3d at 11 (declining "to treat an increased risk of future identity theft as an actual harm for purposes of negligence and breach of fiduciary duty claims based on data breaches"); Colonial Pipeline, *supra* note 37, 2022 U.S. Dist. LEXIS 155295, at *8-11 (alleged increased risk of identity theft by reason of a cyberattack insufficient injury to sustain a negligence claim under Georgia law); Blackbaud II, *supra* note 29, 625 F. Supp. 3d at 997 ("risk of future identity theft [by reason of a cyberattack] is not a compensable harm in Indiana"); Arby's, *supra* note 31, 2018 U.S. Dist. LEXIS 131140, at *40 ("Arby's is correct that a plaintiff may not recover for injuries that are purely speculative, such as the potential risk of future identity theft . . . .").

64. *See supra* note 28.

action,[65] the courts' differing rulings arise not by reason of the facts differing from case to case, but rather from the courts' differing understandings of the injury element of a common-law negligence claim under the relevant state law.[66]

In short, as has occurred with regard to the *economic* injuries typically alleged in a cyberattack class action, the U.S. courts' rulings to date have likewise created a jurisprudential quagmire on the question whether the *non-economic* injuries typically alleged in a cyberattack class action (be they of the "impactful" or the "non-impactful" variety) are actionable in common-law negligence.

So what accounts for this quagmire? The explanation requires going back in time to the "traditional" 20th century tort law principles that this author studied in law school fifty years ago. Under those traditional principles, the tort of negligence existed to "give[] protection against other words, [while] negligence m[ight] result in liability for personal injury or property damage," traditionally no liability attached to negligent conduct that resulted in purely economic or purely emotional injuries, i.e., economic or emotional injuries not associated with physical injury to one's person or tangible property.[67] These traditional principles are reflected in the *Restatement (Second) of Torts* volume on Negligence, published by the American Law Institute in 1965.[68]

---

65. *See supra* Parts I.A and I.B.1.

66. *See* cases cited in notes 60-63 *supra* (all finding the injury in question to be as a matter of law either actionable, or non-actionable, under the state law the court viewed to be applicable to the negligence claim being asserted in the cyberattack class action in question).

67. *Id*.

68. *See* Restatement (Second) of Torts § 436A (Am. L. Inst. 1965) (hereinafter "Second Torts Restatement") (no liability in negligence for standalone

However, as the 20th century waned and the 21st century arrived, U.S. courts began, on occasion, to make certain exceptions to those traditional principles by here and there allowing negligence claims to be predicated on "standalone" economic or emotional injury in circumstances that those courts deemed worthy of protection against negligent conduct from a policy perspective.[69] But these exceptions were made episodically and sporadically, not in response to some sort of nationwide doctrinal shift in the common law of negligence. Nor did these episodically and sporadically created exceptions (at least not immediately) congeal into generally accepted doctrinal principles that U.S. courts could readily look to in evaluating the legal sufficiency of negligence claims that were predicated on non-traditional injuries of this sort.

In the midst of this legal ferment, cyberattack class actions arrived on the litigation scene in the early 21st century. This new species of class action litigation regularly featured negligence claims, but the complaints in cyberattack class actions *never*

---

emotional harm); Restatement (Third) of Torts: Liability for Economic Harm § 1, Reporters Notes, comment a (Am. Law Inst. 2020) (hereinafter "Economic Harm Restatement") (liability in negligence for standalone economic harm wholly unrecognized in the Second Torts Restatement and unintentional infliction of such harm could create liability only under the separate torts of negligent interference with contract or prospective contractual relations and negligent misrepresentation).

69. *See* Economic Harm Restatement, *supra* note 26, § 1, Reporters Notes, comment a ("Liability [in negligence for the unintentional infliction of economic loss emerged only within the last 40 years [*i.e.*, after 1980] as a distinct topic for analysis within the law of torts.); Restatement (Third) of Torts: Liability for Physical and Emotional Harm § 4, comment d (Am. L. Inst. 2010) (hereinafter "Physical/Emotional Harm Restatement") ("The Second Restatement of Torts did not recognize a claim for negligently inflicted emotional harm. Since that Restatement, courts have liberalized the rules for recovery for stand-alone emotional harm.").

predicated such claims on the physical injuries to one's person or tangible property that negligence law had traditionally protected. Instead, such complaints *always* predicated their negligence claims on standalone economic injuries and/or standalone emotional injuries of the sort that negligence law had traditionally eschewed. From their inception then, and continuing to the present, cyberattack class actions have *always* required the presiding court to decide the novel legal question of whether the complaint's ubiquitous negligence claim could be founded on standalone economic and/or emotional injuries. Lacking guidance from any generally accepted doctrinal principles that reflected the judicial ferment that had been occurring in this area of negligence law during the past half-century, the U.S. courts quite predictably stumbled, issuing the slew of conflicting rulings on this question that created the jurisprudential quagmire described above in Part I of this Article.

Meanwhile, as that quagmire was being created, the American Law Institute had underway a project to update the *Restatement (Second) of Torts* to reflect the developments in American tort law since 1965. That project has now largely, though not entirely, been completed. As shown below in Part II of this article, the already-completed portions of that project offer the U.S. courts a set of coherent principles by which to reach consistent decisions, going forward, as to what injuries typically alleged in a cyberattack class action are actionable in negligence.

II. HOW THE THIRD TORTS RESTATEMENT OFFERS COHERENT PRINCIPLES FOR REACHING CONSISTENT DECISIONS AS TO WHAT INJURIES TYPICALLY ALLEGED IN A CYBERATTACK CLASS ACTION ARE ACTIONABLE IN NEGLIGENCE

The American Law Institute ("ALI") describes itself as "the leading independent organization in the United States producing scholarly work to clarify, modernize, and otherwise

improve the law."[70] It is best known for its "restatements" of the law, which are intended to set forth "clear formulations of common law and its statutory elements or variations and reflect the law as it presently stands or might appropriately be stated by a court."[71] "Restatements are primarily written for judges, to help judges understand an area of law and to aid judicial decision making."[72]

"Restatements thus assume a body of shared doctrine enabling courts to render their judgments in a consistent and reasonably predictable manner."[73] They therefore seek to "scan an entire legal field and render it intelligible by a precise use of legal terms."[74] A primary goal of restatements is to address scenarios—such as the one described in Part I of this article—where "the underlying principles of the common law ha[ve] become obscured by the ever-growing mass of decisions in the many different jurisdictions, state and federal, within the United States."[75] Restatements thus seek to "discern the underlying principles that gave [the legal subject] coherence and thus restore the unity of the common law as properly apprehended."[76] In addition to promoting uniformity in the common law, restatements "are also intended to reflect the flexibility and

70. *See* Am. L. Inst., *About ALI* (hereinafter "About ALI"), available at https://www.ali.org/about-ali.

71. *See* Am. L. Inst, Capturing the Voice of The American Law Institute: *A Handbook for ALI Reporters and Those Who Review Their Work* (rev. ed. 2015) (hereinafter "ALI Style Manual"), at 3.

72. About ALI, *supra* note 71.

73. ALI Style Manual, *supra* note 72, at 4.

74. *Id*. at 5.

75. *Id*. at 4.

76. *Id*. at 4.

capacity for development and growth of the common law."[77] Thus, "[a] significant contribution of the [r]estatements has also been anticipation of the direction in which the law is tending and expression of that development in a manner consistent with previously established principles."[78]

Formally, restatements are mere "secondary sources" or "persuasive authorities," as the ALI itself readily acknowledges.[79] Functionally, however, restatements are so persuasive that they have become more of what might be called "quasi-primary" in their authoritativeness. As recently explained by one leading commentator:

"Owing in large part to the prominence of the ALI's membership, which comprises innumerable members of the state and federal judiciaries who actively participate in the working of the organization, Restatements are treated by courts as much more than just persuasive. Their influence (or authoritativeness, so to speak) emerges not merely (or even) from the substantive content of their directives but instead from a significant amount of trust and faith that is placed in the institutional process through which they are produced. That process includes the composition of the organization's membership, which is seen to be representative of the legal profession. In an important sense, therefore, Restatements are functionally imbued with decisionist authority, in which the legitimacy of the organization and the production processes drive the authoritativeness of the content.

77. *Id*. at 5

78. *Id*.

79. Am. L. Inst., *Frequently Asked Questions*, https://www.ali.org/about-ali/faq ("ALI's publications are persuasive authorities, not controlling law . . . [and] serve as useful secondary sources to aid interpretation, advance understanding more generally, or provide a basis for legislation.").

This renders their authority closer to that of a primary source functionally even if not formally."[80]

Owing to their uniquely, and extraordinarily, persuasive nature, ALI restatements are cited thousands of times each year by courts, and courts in every state have relied on a restatement at some point when developing state common law.[81]

The ALI's torts restatements have been particularly influential.[82] For example, the ALI's *Restatement (Second) of Torts* (the "Second Torts Restatement"), the first volume of which was published sixty years ago, in 1965, has had its formulations of the litigation privilege, the tort of intentional infliction of emotional distress, and the doctrine of strict products liability adopted in nearly every state.[83] The *Restatement (Third) of Torts* (the "Third Torts Restatement") is the ALI's multi-decade project to replace and supersede the now sixty-year-old Second Torts Restatement. Like the Second Torts Restatement, which comprises four volumes, the Third Torts Restatement is envisioned as a multi-volume project that, viewed as a whole, will cover the entirety of tort law. Several of the Third Torts

80. Shyamkrishna Balganesh, *Relying on Restatements*, 122 COLUM. L. REV. 2119, 2132 (2022).

81. V. Schwartz & C. Appel, *The Restatement (Third) of Torts Proposes Abandoning Tort Law's Present Injury Requirement to Allow Medical Monitoring Claims: Should Courts Follow?*, 52 SW. L.R. 512, 514 (2024).

82. *Id*.

83. *See id.* and cases cited therein at notes 9 & 10.

Restatement's volumes have already been completed.[84] Others are still in the course of being drafted.[85]

If past is prologue, then there is every reason to expect the Third Torts Restatement to become just as influential in the U.S. courts as are ALI restatements generally and as was the Second Torts Restatement in particular. Indeed, the initial returns from the U.S. courts on the earliest published volumes in the Third Torts Restatement series strongly suggest that will be the case.[86]

---

84. Specifically, the ALI has published, as parts of the Third Torts Restatement, single volume restatements on the following topics: Products Liability (1998), Apportionment of Liability (2000), Liability for Physical and Emotional Harm (2010), and Liability for Economic Harm (2020).

85. Yet to be completed are the Third Tort's Restatement's volumes on Intentional Torts to Persons, Remedies, Medical Malpractice, Miscellaneous Provisions, and Defamation and Privacy. However, with the exception of the Defamation and Privacy volume, the ALI has published so-called "Tentative Drafts" of each of these additional volumes, which drafts (per the ALI) "may be cited as representing the Institute's position until the official text is published." *See, e.g.,* ALI's commentary on Tentative Draft No. 6 of the Third Torts Restatement's volume on Intentional Torts to Persons, available at www.ali.org/publications/restatement-law-third/torts-intentional-torts-persons.

86. *See*, *e.g.* Carroll v. Carnival Corp., 955 F.3d 1260, 1268 (11th Cir. 2020) (adopting the Third Torts Restatement's view that proof that a danger was open and obvious to the plaintiff does not inherently negate a negligence claim based on the defendant's failure to warn the plaintiff of the danger, but should instead be treated as a factor in the ultimate analysis); Wurster v. Plastics Grp., Inc., 917 F.3d 608, 617 (8th Cir. 2019) (adopting the Third Torts Restatement's four-factor test for determining a post-sale duty to warn); Berrier v. Simplicity Mfg., 563 F.3d 38, 41-44 (3d Cir. 2009) (relying on the Third Torts Restatement in broadening strict liability in products liability cases from users or consumers of a commercial product to anyone harmed by a defective product); Nelson v. Metro-North Commuter R.R., 235 F.3d 101, 106-107 (2d Cir. 2000) (applying the Third Torts Restatement to decide that the harm alleged in a claim of negligent infliction of emotional distress by an employee against her employer should be judged by the severity of what may have

As discussed below in this Part II, two of the more recently published volumes in the series—*Liability for Physical and Emotional Harm* (published in 2010), and *Liability for Economic Harm* (published 2020)—contain detailed provisions on what sort of "injury" can sustain a tort claim, including in particular, a claim in common-law negligence. If, as there is every reason to expect, those provisions come to be widely adopted by the U.S. courts, they will (as discussed below in Part II) enable the U.S. courts to begin to come to consistent and coherent answers to what has to date, as shown in Part I of this article, been the vexing question of what sorts of injuries typically alleged in a class action based on a cyberattack can sustain a claim in common-law negligence based on that attack.[87]

happened, rather than actual events); Foster v. Costco Wholesale Corp., 128 Nev. 773, 775 (2012) (adopting the Third Torts Restatement's notion that landowners are not exempt from potential premises liability due simply to the open and obvious nature of a danger on their property); Franks v. Coopersurgical, Inc., 722 F. Supp. 3d 63, 92 (D.R.I. 2024) (applying the Third Torts Restatement's learned intermediary doctrine in a products liability case wherein the doctor was in a better position to warn a patient about potential dangers of medical equipment manufactured by a defendant).

87. Indeed, a few U.S. courts have already had occasion to apply the provisions in these more recently published volumes in the context of cyberattack class actions. *See*, in addition to the cases discussed in notes 101 and 106 *infra*, Charlie v. Rehoboth McKinley Christian Health Care Servs., 598 F. Supp. 3d 1145, 1154-55 (D.N.M. 2022) (applying Section 7 of the *Liability for Physical and Emotional Harm* volume of the Third Torts Restatement to determine whether the defendant owed the plaintiff a duty of care in common-law negligence to protect the plaintiff's personal information against a cyberattack).

A. Liability in Negligence for Economic Harm Caused by a Cyberattack: Teachings of the Third Torts Restatement

Part II.A.1 below summarizes the Third Torts Restatement's general principles regarding liability in negligence for "economic harm." Part II.A.2 below then applies those general principles to the types of economic harm typically alleged in a class action based on a cyberattack and shows that, under those general principles, such types of economic harm are inactionable as a matter of law in common-law negligence, according to the Third Torts Restatement.

1. The Third Torts Restatement's Principles Regarding Liability in Negligence for Economic Harm

The Third Torts Restatement's principles regarding liability in negligence for "economic harm" are, for the most part, set forth in Sections 1-8 of the *Liability for Economic Harm* volume of the Third Torts Restatement (the "Economic Harm Restatement").[88] For purposes of the Economic Harm Restatement, "economic loss" (which term is used interchangeably with the terms "economic injury," "economic harm," and "economic damages" in the Third Torts Restatement) means "pecuniary damage not arising from injury to the plaintiff's person or from physical harm to the plaintiff's property."[89] In the cyberattack class action context, of course, the plaintiff's injuries are never alleged to have arisen from injury to the plaintiff's person or from physical harm to the plaintiff's property, so for purposes of the alleged injuries that are within the scope of this article "economic harm" means simply "pecuniary damage," which the Third Torts Restatement elsewhere defines to mean "items

88. *See* Economic Harm Restatement, *supra* note 26, §§ 1-8.

89. *Id*, § 2.

of damages for which a market exists and that therefore can be valued by reference to the market valuation."[90]

The Third Torts Restatement imposes substantial limits on a plaintiff's ability to predicate a negligence claim on "economic harm" as therein defined. For starters, Section 1 of the Economic Harm Restatement provides that "[a]n actor has no general duty to avoid the unintentional infliction of economic loss on another." Section 3 then takes that general principle a step further by negating "liability in tort for economic loss caused by negligence in the performance or negotiation of a contract between the parties" except where the Economic Harm Restatement otherwise provides.[91] Consistent with the general rule of Sections 1 and 3 prohibiting economic harm from being actionable in common-law negligence, the Economic Harm Restatement expressly limits recovery for economic loss in common-law negligence to the circumstances specified in Sections 2 through 8.[92] Those sections then identify four and only four circumstances under which, notwithstanding the general principle set forth in Sections 1 and 3, economic harm *can* be the foundation of a common-law negligence claim: professional malpractice[93]; negligent misrepresentation[94]; negligent performance of services[95]; and public nuisance.[96]

---

90. *See* Apportionment of Liability Restatement, *supra* note 7, § E18, comment c (defining "economic damages").

91. *Id.* § 3.

92. Economic Harm Restatement, *supra* note 26, § 1.

93. *Id.* § 4.

94. *Id.* § 5.

95. *Id.* § 6.

96. *Id.* § 8.

As shown in Part II.A.2 below, none of these four exceptions would cover the types of economic harm typically alleged in a class action based on a cyberattack. A court applying the Third Torts Restatement to a negligence claim advanced in a cyberattack class action should therefore dismiss the claim as a matter of law insofar as it is founded on economic harm allegedly suffered by the individuals whose personal information was involved in the attack.

2. Application of the Third Torts Restatement's Principles to Negligence Claims Based on Economic Harm Allegedly Caused by a Cyberattack

As discussed in Part I.A above, the types of economic harm alleged by plaintiffs in cyberattack class actions in support of their complaint's common-law negligence claim typically include some or all of such items as (1) out-of-pocket costs of fraud and other identity theft perpetrated by means of personal information stolen in the cyberattack; (2) expenses of measures taken to prevent such fraud and other identity theft from occurring; (3) diminution, by reason of the theft and consequent availability of the personal information in question, in the market value of that information; and (4) overpayment for the product or service purchased from the entity that suffered the cyberattack in question, or underpayment for employment services rendered to that entity, by reason of the entity's failure to provide the promised or otherwise legally required security for the personal information involved in the cyberattack.[97] Each of these items represents "pecuniary damages,"[98] i.e., "items of damages for which a market exists and that therefore can be valued by

97. *See supra* notes 19-22 and accompanying text.

98. Economic Harm Restatement, *supra* note 26, § 2.

reference to the market valuation."[99] As such, each such item falls squarely within the Third Torts Restatement's definition of "economic loss" and thus is actionable in common-law negligence under the Third Torts Restatement if and only if it is sought by means of a claim that fits within one of the four exceptions to the Third Torts Restatement's general rule that economic loss is not actionable in common-law negligence.[100]

None of those four exceptions would apply, however, in the context of a negligence claim asserted in a cyberattack class action. For starters, the professional malpractice and public nuisance exceptions laid out in Sections 4 and 8 of the Economic Harm Restatement[101] are plainly inapposite, as no claim could be made that the cybersecurity measures employed by an entity that suffered a cyberattack constituted either professional

99. *See* Apportionment of Liability Restatement, *supra* note 7, § E18, comment c (defining "economic damages").

100. *See* Southern Indep. Bank v. Fred's, Inc., 2019 U.S. Dist. LEXIS 40036, at *41-42 (M.D. Alab. Mar. 13, 2019) (under the Third Torts Restatement, economic losses are not recoverable in a cyberattack class action unless one of the exceptions to the Economic Harm Restatement's economic loss doctrine applies).

101. *See supra* notes 94 and 97 and accompanying text.

malpractice[102] or a public nuisance[103], as claims of that sort are defined by the Economic Harm Restatement.

---

102. In regard to the "professional malpractice" exception, while "professionals" such as doctors, lawyers, and accountants can and do suffer cyberattacks, those professionals' cybersecurity measures in regard to their clients' personal information would not be services within the "professional" expertise of those professionals and thus could not sustain a professional malpractice claim. See Economic Harm Restatement, *supra* note 26, § 4, comment c (defining standard of care for purposes of the professional malpractice exception as "to exercise the skill and employ the knowledge normally possessed by members of the profession in similar circumstances"); *cf.* Wengui v. Clark Hill, PLC, 440 F. Supp. 3d 30, 38 (D.D.C. 2020) (upholding legal malpractice claim against law firm based on law firm's alleged lax data security practices that ostensibly allowed a cyberattack, but without considering whether employing legally required data security measures fell within the law firm's professional expertise, as required to state a legal malpractice claim under the Third Torts Restatement). Nor could a professional malpractice claim be asserted against a cybersecurity firm that ostensibly enabled a cyberattack by negligently advising the entity that suffered the attack regarding the cybersecurity measures it should employ to prevent such an attack; such firms do not meet the definition of "professional" for purposes of the professional malpractice exception, as the occupation of such firms does not require formal training and a license issued by a public body and does not have an internal code of conduct and discipline. *See* Economic Harm Restatement, *supra* note 26, § 4, comment b (so defining "professional" for purposes of the professional malpractice exception). *Compare* Music Group Macao Commercial Offshore Ltd. v. Foote, 2015 U.S. Dist. LEXIS 81415, at *53-54 (N.D. Cal. June 22, 2015) (after noting that "no court has found that a person performing in Defendant's role [as the company's Chief Technology Officer] owes a duty to perform at a particular level of care such that an individual performing such role owes a professional duty to use such skill, prudence and diligence as other members of the profession commonly possess and exercise," and expressing skepticism as to whether such a duty could be established, the court allowed the plaintiff's professional malpractice claim to go forward on the ground that the question of whether the defendant owed such a professional duty was for the jury to decide) *with* Economic Harm Restatement, *supra* note 26, § 4, comment b (question of whether

Nor could a negligence claim in a cyberattack class action be shoehorned into the negligent misrepresentation or the negligent provision of services exceptions set forth in Sections 5 and 6 of the Economic Harm Restatement. To begin with, those exceptions are entirely unavailable to individuals who are in privity with the defendant where the defendant's alleged negligence occurred in the course of performing the parties' contract.[104] This limitation makes these exceptions unavailable to the vast majority of individuals who might claim to have suffered economic harm from a cyberattack by reason of the defendant's allegedly negligent cybersecurity-related misrepresentations or services, as a defendant's negligent misrepresentations to another regarding its cybersecurity measures, or negligent provision to another of cybersecurity services, would nearly always only occur in a contractual setting where the parties' contract was a but-for cause of the plaintiff' alleged economic losses and that contract therefore barred a claim in negligence for those losses

---

a professional duty is owed for purposes of this exception "is a decision for the court").

103. "A public nuisance arises when a defendant's wrongful act causes harm to a public right: a right held in common by all members of the community." Economic Harm Restatement, *supra* note 26, § 8. This would never be the case in the cyberattack context, where the defendant's alleged wrongful act allegedly causes harm only to, and allegedly infringes the legal rights only of, the individuals whose personal information was involved in the cyberattack in question—not to, or of, the community at large.

104. *See* Economic Harm Restatement, *supra* note 26, § 5(5) ("[t]his Section does not recognize liability for negligent misrepresentations made in the course of negotiating or performing a contract between the parties") and § 6(4) ("[t]his Section does not recognize liability for negligence in the course of negotiating or performing a contract between the parties").

under either Section 5 or Section 6 of the Economic Harm Restatement.[105]

---

105. In Weisenberger v. Ameritas Mutual Holding Co., 597 F.Supp.3d 1351 (D. Neb. 2022), the court held that § 6(4) did not preclude a negligence claim based on an insurer's alleged failure to protect its insureds' personal information against a cyberattack, reasoning that § 6(4) would be operative only if the parties' insurance contract indisputably contractually obliged the insurer to exercise reasonable care to protect its insureds' personal information. *See* 597 F.Supp.3d at 1361 n.3. But the Economic Harm Restatement makes clear that § 6(4) does not make a negligence claim available merely because the parties' contract does not itself impose liability for the defendant's challenged conduct. Economic Harm Restatement, *supra* note 26, § 3, comment c ("A contract can allocate a risk without mentioning it explicitly; silence may itself serve as an allocation if the risk falls within the scope of activity the contract governs."); *see* Sheen v. Wells Fargo Bank, N.A., 12 Cal. 5th 905, 933-34 (Cal. 2022) ("Sheen") (holding, in reliance on Section 3 of the *Economic Harm Restatement*, that "[t]he better view, however, is that there does not need to be a viable breach of contract claim for the economic loss rule to apply" when the parties are in privity). Instead, the correct inquiry under Section 3 is whether the negligence claim "arises under" – rather than being independent of – the parties' contract, *i.e.*, it "arise[s] precisely because the parties are in a preexisting contractual relationship." *Id.* at 934-35. Thus, where a negligence claim seeks monetary losses that would not have arisen but for a contract between the parties, that contract "displaces the obligations of §§ 5 and 6; [and] the contract alone determines the parties' responsibility for economic loss caused by negligence in performing it." Economic Harm Restatement, *supra* note 26, § 3, comment h.

In *Weisenberger*, "the defendant gathered PII incident to performing a service: that is, considering the plaintiff's application for (and acceptance of) insurance benefits," and allegedly "was obliged to exercise reasonable care when performing" that service. 597 F.Supp.3d at 1361. Thus, as would be the case in any cyberattack-based negligence claim based on an alleged failure to protect personal information collected by the defendant pursuant to its contract with the plaintiff, the negligence claim in *Weisenberger* by its very terms arose because of, and sought to recover monetary losses that would not have arisen but for, the parties' contract. As such, the negligence claim in *Weisenberger* should have been found precluded by § 6(4) regardless of whether the

As for individuals who do not have a contract with the defendant that precludes them from pursuing such a claim, the negligent misrepresentation exception offers them the opportunity to base a negligence claim on economic harm only where the alleged misrepresentation was made "for the[ir] guidance"; where the alleged economic harm was "caused to them by their reliance upon" that misrepresentation; and where such reliance occurred "in a transaction that the [defendant] intend[ed] to influence."[106] In like fashion, the negligent provision of services exception offers such individuals such an opportunity only where the allegedly deficient service was "perform[ed] . . . for their benefit"; where the alleged economic harm was "caused to them by their reliance upon the service"; and where such reliance occurred "in a transaction that the [defendant] intend[ed] to influence."[107] In the cyberattack context, it is extremely difficult to conceive of a scenario where: (1) the defendant made or performed cybersecurity-related statements or services for the

parties' contract-imposed liability for the cyberattack on the defendant. *See* Terpin, *supra* note 29, 118 F.4th at 1116 (relying on *Sheen* and Section 3 of the Economic Harm Restate*ment* to dismiss cyberattack-based negligence claim under California economic loss doctrine because "[defendant] had access to [plaintiff]'s customer information through its contractual relationship with him"); Ace Am. Ins. Co. v. Accellion, Inc., 2022 U.S. Dist. LEXIS 119232, at *19 (N.D. Cal. Apr. 11, 2022) (relying on Section 3 of the *Economic Harm Restatement* to dismiss cyberattack-based negligence claim under California economic loss doctrine where, as in *Weisenberger*, plaintiff had acknowledged that its "negligence claims all arise out of [defendant's] negligent performance of its service obligations under the [parties'a]greement").

106. *See* Economic Harm Restatement, *supra* note 26, §§ 5(1) and 5(2)(b).

107. *See Id*, §§ 6(1) and 6(2)(b). *See also* Economic Harm Restatement, *supra* note 26, § 6, comment a (emphasizing the close relationship of the negligent provision of services exception to the negligent misrepresentation exception and the intention that liability under the former exception be limited to the same extent as liability is limited under the latter exception).

guidance or benefit of the plaintiff; *and* (2) the plaintiff incurred economic harm in reliance on such cybersecurity-related statements or services; *and* (3) such reliance occurred in the context of a transaction that the defendant intended to influence between the plaintiff with someone other than the defendant; *and* (4) all this somehow occurred even though the parties themselves had no contractual relationship that barred the plaintiff from seeking to recover such harm from the defendant on a negligent misrepresentation or negligent provision of services theory. It is consequently extremely difficult to imagine how a cyberattack class action complaint could ever plausibly make such allegations, as it would have to in order to successfully invoke either the negligent misrepresentation exception or the negligent provision of services exception on behalf of individuals whose personal information was stolen in a cyberattack.[108]

---

108. Even if a case could be imagined where a named plaintiff in a cyberattack class action both had no claim-precluding contractual relationship with the defendant and in fact *could* make the allegations necessary to bring either the negligent misrepresentation exception or the negligent provision of services exception into play (and, again, the author of this article has been unable to conjure up such a case), such a named plaintiff almost certainly never *would* make those allegations in an effort to sustain his or her negligence claim. That is because any individual seeking to invoke either of these exceptions would have to prove that he or she *in fact* relied on the cybersecurity-related statements or services that the defendant allegedly made or performed for his or her guidance or benefit and that he or she *in fact* suffered economic harm as a result of such reliance. In the class action context, class-wide proof could not be used to establish such reliance and such economic harm on the part of all the class members; instead, an individualized member-by-member inquiry would be required to determine whether any given class member had in fact engaged in the reliance and suffered the consequent economic harm necessary to establish the defendant's liability for such harm in common-law negligence by means of either the negligent misrepresentation exception or the negligent provision of services exception. Where, as would therefore be the case here, individualized inquiries of the class

And, indeed, those few cyberattack class action complaints that have attempted to invoke the negligent misrepresentation exception have for the most part been dismissed for failure to make the allegations necessary to invoke that exception.[109] Today, the typical cyberattack class action complaint includes no such allegations when it advances a negligence claim on behalf of individuals whose information was stolen in the cyberattack in question.[110]

---

members would be required to establish the defendant's liability to those class members on the claim being asserted, the claim is not suitable for class certification. *See* Sampson v. United Servs. Auto. Ass'n, 83 F.4th 414, 421-23 (5th Cir. 2023) and Lara v. First Nat'l Ins. Co. of Am., 25 F.4th 1134, 1138-40 (9th Cir. 2022) (both holding that Rule 23(b)(3) predominance could not be shown where an element necessary to establish liability on the claim in question, such as injury, could not be proven by means of class-wide evidence). As a result, there would be no point in the named plaintiff in a cyberattack class action trying to invoke either the negligent misrepresentation exception or the negligent provision of services exception, even assuming he or she theoretically could.

109. *See, e.g.*, Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162, 177-78 (3d Cir. 2008) (affirming district court's dismissal of negligence claim in cyberattack class action under Pennsylvania's economic-loss rule for failure to plead the elements on the negligent-misrepresentation exception as specified in Section 552 of the Second Torts Restatement, the highly similar predecessor to Section 5 of the Economic Harm Restatement); Longenecker-Wells v. Benecard Servs., 2015 U.S. Dist. LEXIS 126837, at *13-17 (M.D. Pa. Sept. 22, 2015) (same holding as *Sovereign Bank*, cited earlier in this footnote); *cf.*, In re Zappos.com, Inc., 2013 U.S. Dist. LEXIS 128155, at *16-19 (D. Nev. Sept. 9, 2013 (upholding, under Nevada law, plaintiffs' invocation in cyberattack class action of negligent-misrepresentation exception to economic-loss rule to sustain their complaint's negligence claim, based on court's conclusion that under Nevada law the exception applies whenever the parties are not in privity).

110. The UnitedHealth Complaint, *supra* note 2, is a case in point. The named plaintiffs in that complaint were not allegedly in privity with the defendants; indeed, that complaint nowhere alleges that the plaintiffs even

Finally, by their express terms the negligent misrepresentation and negligent provision of services exceptions are available to make economic harm actionable in negligence only where the plaintiff is "the person or one of a limited group of persons" for whose guidance or benefit the defendant made the statement or performed the service in question.[111] This limitation is intended "to prevent a defendant's potential liability from becoming indeterminate and unduly widespread,"[112] as would be the case, for example, in a claim brought by investors in a publicly traded company based on a third-party accountant's negligent misrepresentation regarding the company's financial health.[113] Cyberattack class actions are, by definition, *always* brought on behalf of a group of individuals that is so numerous that it would be "impracticable" for all the individuals in the group to

---

knew that the defendants were in possession of the personal information of theirs that was involved in the cyberattack at issue. Rather, as is usually the case where a cyberattack class action is brought against a defendant that had no direct interaction or relationship with the individuals whose information was involved in the attack, the named plaintiffs in the UnitedHealth Complaint provided the personal information at issue to third parties (here, health insurers and/or healthcare providers), who in turn (unbeknownst to the named plaintiffs) provided the information to the defendants (here, for assistance in administering health insurance claims). *Id.* ¶¶ 157-167. The UnitedHealth Complaint's negligence claim therefore does not make, and indeed could not have made, the allegations necessary for that claim to pass muster under the Third Torts Restatement's negligent misrepresentation exception or its negligent provision of services exception insofar as the claim is predicated on the economic harm the named plaintiffs allegedly suffered by reason of the cyberattack. *See id.* ¶¶ 397-415.

111. *See* Economic Harm Restatement, *supra* note 26, §§ 5(2)(a) and 6(2)(a).

112. *Id*, § 5, comment f.

113. *Id*, § 5, Illustration 7.

be joined as plaintiffs in the action.[114] Cyberattack class actions are, therefore, *never* brought on behalf of the sort of "limited group of persons" envisioned by these two exceptions. For this further reason, then, such class actions are always incapable of satisfying either the negligent misrepresentation exception or the negligent provision of services exception to the Third Torts Restatement's general rule that economic harm is not actionable in common-law negligence.

In short, a court applying the principles of the Third Torts Restatement to a negligence claim asserted in a cyberattack class action complaint should apply the Third Torts Restatement's general rule that economic harm cannot sustain a claim in common-law negligence, as none of the recognized exceptions to that rule would apply in such an action. Such a court should therefore reject such a claim as a matter of law insofar as the complaint seeks to satisfy the injury element of the claim by relying on alleged economic harm that the plaintiff(s) incurred by reason of the cyberattack at issue.

B. Liability in Negligence for Non-Economic Harm Caused by a Cyberattack: Teachings of the Third Torts Restatement

Part II.B.1 below summarizes the Third Torts Restatement's general principles regarding liability in negligence for "non-economic harm." Part II.B.2 below then applies those general principles to the types of non-economic harm typically alleged in a

114. FED. R. CIV. P. 23(a)(1) (an action may be maintained as a class action "only if . . . the class is so numerous that joinder of all members is impracticable"). For example, the class in *Weisenberger* (discussed *supra* note 106) consisted of "at least 39,675 of the defendant's customers." 597 F.Supp.3d at 1356. The *Weisenberger* court took no account of the "limited group of persons" requirement, however, in allowing the plaintiff's negligence claim to go forward under Section 6 of the Economic Harm Restatement. *Id.* at 1361.

cyberattack class action and shows that, under those general principles, such types of non-economic harm are inactionable as a matter of law in common-law negligence, according to the Third Torts Restatement.

1. The Third Torts Restatement's Principles Regarding Liability in Negligence for Non-Economic Harm

The Third Torts Restatement recognizes liability in common-law negligence for two, and only two, types of "non-economic harm," *i.e.*, harm that does not meet the Third Torts Restatement's, and this article's, definition of "economic harm."[115] Those two types of non-economic harm—namely, "physical harm" and "emotional harm"—are addressed in the Third Torts Restatement's volume entitled *Liability for Physical and Emotional Harm* (the "Physical/Emotional Harm Restatement").[116]

Under Section 4 of the Physical/Emotional Harm Restatement, "physical harm" means "the physical impairment of the human body ('bodily harm') or of real property or tangible personal property ('property damage')" and "[b]odily harm includes physical injury, illness, disease, impairment of bodily function, and death."[117] Cyberattacks never cause, and as a result cyberattack class action complaints never allege, "physical harm" on the part of the individuals whose personal

115. *See supra* text accompanying notes 7 (defining "economic harm" for purposes of the Third Torts Restatement, and for purposes of this article, as injuries with respect to which a market exists (at least allegedly) and that therefore can be valued by reference to the market valuation) and 11-13 (defining "non-economic harm" for purposes of this article to mean any alleged harm that is not within the Third Torts Restatement's and this article's definition of "economic harm").

116. *See* Physical/Emotional Harm Restatement, *supra* note 70, §§ 45-48.

117. *Id.* § 4.

information was involved in the attack. As a result, this article need not, and does not, explore what sorts of injuries do and do not constitute "physical harm" within the meaning of the Third Torts Restatement.

Section 4 of the Physical/Emotional Harm Restatement defines "emotional harm" to mean "impairment or injury to a person's emotional tranquility."[118] The term "encompasses a variety of mental states, including fright, fear, sadness, sorrow, despondency, anxiety, humiliation, depression (and other mental illnesses), and a host of other detrimental—from mildly unpleasant to disabling—mental conditions."[119] Whereas "[m]ost physical harm, with the exception of disease, results from traumatic impact" with the body or property in question, "emotional harm can occur without such trauma, indeed without any event that resembles a physical-harm tort."[120] As a result, while physical harm "usually provides objective evidence of its existence and extent, . . . the existence and severity of emotional harm is usually dependent upon the report of the person suffering it or symptoms that are capable of manipulation or multiple explanations."[121]

---

118. *Id.* § 45.

119. *Id.* § 45 comment a. *See also* Apportionment of Liability Restatement, *supra* note 7, § E18, comment c ("[n]oneconomic damages" includes "damages recoverable for intangible harms that are not susceptible to market valuation" such as "pain and suffering, inconvenience, disfigurement, emotional distress, loss of society and companionship, loss of enjoyment of life ('hedonic' damages), loss of consortium other than lost domestic services, injury to reputation, and humiliation").

120. Physical/Emotional Harm Restatement, *supra* note 70, § 45 comment a.

121. *Id.* § 4 comment b; *see also id.* § 45 comment a ("Usually the existence of bodily harm can be verified objectively while the existence and severity of emotional harm is ordinarily dependent on self-reporting.").

The Second Torts Restatement's volume on negligence recognized no liability in negligence for negligently inflicting "standalone" emotional harm, i.e., emotional harm unaccompanied by physical harm.[122] Based on judicial developments subsequent to that volume's publication in 1965, the Physical/Emotional Harm Restatement slightly modified that flat prohibition by (1) first endorsing "a general rule that negligently caused pure emotional harm is not recoverable [in negligence] even when it is foreseeable," and (2) then subjecting that general rule to the two extremely limited exceptions specified in Sections 47 and 48 of the Physical/Emotional Harm Restatement.[123]

By their express terms, the exceptions to that general rule specified Sections 47(a) and 48 of the Physical/Emotional Harm Restatement are available only where the defendant's negligent conduct either "places the [plaintiff] in danger of immediate bodily harm"[124] or "causes sudden serious bodily injury to a third person."[125] As previously noted, cyberattacks never involve, and cyberattack class action complaints never allege anyone was placed in danger of or suffered, "immediate bodily harm" or "sudden serious bodily injury." Accordingly, this article need not and does not address the exceptions that Sections 47(a) and 48 of the Physical/Emotional Harm Restatement make

122. *See* Second Torts Restatement, *supra* note 69, § 436A; Physical/Emotional Harm Restatement, *supra* note 70, § 4 comment d ("The Second Restatement of Torts did not recognize a claim for negligently inflicted emotional harm.") and ch. 8, § Scope ("the Second Restatement provided for no recovery when negligence caused only emotional harm").

123. *See* Physical/Emotional Harm Restatement, *supra* note 70, § 47, comment i ("the rules stated in [§ 47] and in § 48 are exceptions to a general rule that negligently caused pure emotional harm is not recoverable even when it is foreseeable").

124. *Id.* § 47(a).

125. *Id.* § 48.

available to the general rule that standalone emotional harm is not actionable in negligence.

That leaves Section 47(b) of the Physical/Emotional Harm Restatement as the only exception to that general rule that theoretically might make actionable in negligence one or more of the non-economic injuries that are typically alleged in a cyberattack class action. Section 47(b) provides as follows:

"Negligent Conduct Directly Inflicting Emotional Harm on Another

"An actor whose negligent conduct causes serious emotional harm to another is subject to liability to the other if the conduct:

"…

"(b) occurs in the course of specified categories of activities, undertakings, or relationships in which negligent conduct is especially likely to cause serious emotional harm."[126]

By its very terms, then, Section 47(b) makes standalone emotional harm actionable in negligence only if (a) the emotional harm in question was directly caused by an actor's negligent conduct; (b) that emotional harm was serious in nature; and (c) the actor's negligent conduct occurs in the course of specified categories of activities, undertakings, or relationships in which negligent conduct is especially likely to cause serious emotional harm.[127] As shown below in Parts II.B.2.a-c, the non-economic injuries typically alleged in a cyberattack class action fail to meet any of these three requirements. Moreover, Section 47(b) is only intended to cover emotional harm that is not of the sort that is already addressed by the "variety of other torts [that] protect

126. *Id.* § 47.

127. *Id.* § 47(b).

specific aspects of emotional tranquility."[128] As shown below in Part II.B.2.d, the non-economic injuries typically alleged in a cyberattack class action fail to meet this additional fourth requirement because they are the sort of harm that is already addressed by another tort that protects specific aspects of emotional tranquility—namely, the tort of invasion of privacy. As a result, a court applying the Third Torts Restatement to a negligence claim asserted in a cyberattack class action should dismiss the claim as a matter of law insofar as it relies on non-economic injuries to satisfy the injury requirement of such a claim.

2. Application of the Third Torts Restatement's Principles to Negligence Claims Based Non-Economic Harm Allegedly Caused by a Cyberattack.

As discussed above in Part I.B, in cyberattack class actions the non-economic injuries allegedly suffered by the individuals whose personal information was involved in the cyberattack in question typically include (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) emotional and mental distress and anguish resulting from the access, theft and/or posting of their personal information; (4) disruption of their lives; (5) time and effort expended responding to and preventing the threats and harm posed by the cyberattack, and (6) a continued substantial and imminent risk of the misuse of their personal information.[129] The complaints in cyberattack class actions typically assert that each of these non-economic injuries is sufficient to sustain the complaint's common-law negligence claim.[130] As shown in Part II.B.1 above, under the Third Torts

128. *Id.* § 47(b), comment o.

129. *See supra* note 6 and accompanying text.

130. *See supra* note 18 and accompanying text.

Restatement injuries of this sort are actionable in negligence only if (a) the defendant's negligent conduct *directly* causes those injuries to occur; (b) they constitute *serious* emotional harm; and (c) the defendant's negligent conduct occurs in the course of specified categories of activities, undertakings, or relationships in which negligent conduct is *especially likely* to cause serious emotional harm.[131] Also, as further shown in Part II.B.1 above, under the Third Torts Restatement such injuries are actionable in negligence only if (d) they are not the sort of injury *addressed by some other tort* that protects specific aspects of emotional tranquility.[132] As shown below in Parts II.B.2.a-d, the non-economic injuries typically alleged in a cyberattack class action in support of the complaint's negligence claim fail to meet any of these four requirements.

a. No Direct Causation

As reflected in the provision's very title, harm is actionable under Section 47 of the Third Torts Restatement only where it is *directly* caused by the defendant's negligent conduct.[133] In the cyberattack context, however, the injuries allegedly incurred by

131. Physical/Emotional Harm Restatement, *supra* note 70, § 47(b); *see supra* Part II.B.1.

132. *Id*, § 47(b), comment o; *see supra* Part II.B.1.

133. *Id*, § 47 (entitled "Negligent Conduct *Directly* Inflicting Emotional Harm on Another") (emphasis added). *See also id.* ch, 8, Scope ("Section 47 addresses liability for negligently *and directly* inflicting pure emotional harm on another.") (emphasis added). Instead, *indirectly* inflicted emotional harm is actionable in negligence only in the limited circumstances specified in Section 48 of the Physical/Emotional Harm Restatement. As noted above, because that section is available only where the defendant's alleged negligence "causes sudden serious bodily injury to a third person," Section 48 would never make actionable in negligence any of the injuries typically alleged in a cyberattack class action complaint. *See supra* note 126 and accompanying text.

the individuals whose personal information was involved in the cyberattack at issue—be they economic or non-economic in nature—are never *directly* caused by the alleged negligence of the entity that suffered the attack. Rather, those injuries are always *directly* caused by the criminal that perpetrated the attack.[134] Thus, while those injuries might have been reasonably foreseeable by the entity that suffered the cyberattack, and as such might be said to have been *proximately* caused by the alleged negligence of the entity that suffered the attack, they could never be said to have been *directly* caused by that entity's negligence.[135] For this reason alone, then, Section 47(b) would never

134. See "Direct Cause," The Law Dictionary, www.thelawdictionary.org/direct-cause (defining "direct cause" to mean "the phrase that describes the immediate cause of an accident or an injury"); "Direct Cause," The Law Insider, www.lawinsider.com/dictionary/direct-cause (defining "direct cause" to mean "[t]he cause that directly resulted in the event (the first cause in the chain" and "[t]he immediate events or conditions that caused the accident"); "Direct Cause," Justia Legal Dictionary, www.dictionary.justia.com/direct-cause (defining "direct cause" to mean "[t]he immediate event or circumstance that results in a particular consequence or outcome").

135. Indeed, the comments to Section 47 expressly state that alleged harm is not actionable thereunder merely because the harm was a reasonably foreseeable consequence of the defendant's allegedly negligent conduct. *See* Physical/Emotional Harm Restatement, *supra* note 70, § 47, comment i ("Courts often state that the test for determining whether negligently caused emotional harm is recoverable is whether the actor reasonably should have foreseen the emotional harm. But foreseeability cannot appropriately be employed as the standard to limit liability for emotional harm."). As those comments explain, "the rules stated in [§ 47] and in § 48 are exceptions to a general rule that negligently caused pure emotional harm is not recoverable even when it is foreseeable."

make actionable in negligence any of the non-economic injuries typically alleged in a cyberattack class action.[136]

b. No Serious Emotional Harm

By Section 47's own express language, only "serious emotional harm" is actionable thereunder.[137] None of the non-economic injuries typically alleged in cyberattack class actions constitutes "serious emotional harm" within the meaning of Section 47, as shown below.

For starters, consider the customary allegation of a cyberattack class action complaint that the individuals whose personal information was involved in the cyberattack suffered an

136. It would not be persuasive to argue that Section 47's requirement of "direct" causation merely demands that the defendant's negligence must have been a "cause in fact" or a "but-for cause" of the emotional harm at issue. The Physical/Emotional Harm Restatement uses the term "factual cause" to describe the requirement that tortious conduct be a "cause in fact" or a "but-for" cause of an individual's harm for that harm to be actionable. *See* Physical/Emotional Harm Restatement, *supra* note 70, § 26 ("Tortious conduct must be a factual cause of harm for liability to be imposed. Conduct is a factual cause of harm when the harm would not have occurred absent the conduct."); *id.* § 26 comments a and b (explaining that, for purposes of the Physical/Emotional Harm Restatement, "factual causation" means but-for causation and replaces the Second Torts Restatement's "cause-in-fact" requirement). Having expressly adopted the term "factual causation" to refer to but-for causation, the drafters of the Physical/Emotional Harm Restatement would not have used the word "directly" (rather than, say, "factually') in Section 47 to incorporate a but-for causation requirement into that provision. Nor would it have been logical for them to expressly include a but-for causation requirement in Section 47, as Section 26 already independently imposed that causation requirement. Thus, the word "directly" in Section 47 can only reasonably be read to impose an additional, more stringent, causation requirement, above and beyond Section 26's factual cause requirement and Section 29's proximate cause requirement.

137. *Id.* § 47.

"injury" actionable in negligence merely by reason of the criminal who perpetrated the attack having gained unauthorized access to that information, and regardless of what the attacker did with that information or whether the individuals in question ever even became aware of that unauthorized access.[138] The Physical/Emotional Harm Restatement's definition of "emotional harm" is, to be sure, quite broad, but it does require *some* "impairment or injury to a person's emotional tranquility."[139] Plainly an event or circumstance of which an individual has no awareness at all cannot cause any impairment—even a "mildly unpleasant"[140] one—to a person's emotional tranquility. As a result, the mere unauthorized access to one's personal information in a cyberattack can never in and of itself constitute "emotional harm" that might theoretically be actionable in negligence under the Physical/Emotional Harm Restatement. And since such unauthorized access also can never by itself constitute either "physical harm"[141] or "economic harm"[142]—the only

138. *See, e.g.*, UnitedHealth Complaint, *supra* note 2, at Count I ("Negligence"), ¶ 413 (asserting that individuals whose personal information was stolen in the Change Health cyberattack thereby suffered "(1) loss of privacy; [and] (2) misappropriation of their identity, name and likeness," which "injuries" are actionable in negligence).

139. Physical/Emotional Harm Restatement, *supra* note 70, § 45.

140. *Id.* § 45, comment a (noting that the mental states encompassed by the term "emotional harm" include "all detrimental—from mildly unpleasant to disabling—mental conditions").

141. *Id.* § 4 (defining "physical harm" as "the physical impairment of the human body ('bodily harm') or of real property or tangible personal property ('property damage')").

142. Economic Harm Restatement, *supra* note 26, § 2 (defining "economic loss" as "pecuniary damage not arising from injury to the plaintiff's person or from physical harm to the plaintiff's property"); Apportionment of Liability Restatement, *supra* note 7, § E18, comment c (defining "economic

two other types of injury that are ever actionable in negligence under the Third Torts Restatement —it necessarily follows that such unauthorized access never in and of itself constitutes an injury that is actionable in common-law negligence under the Third Torts Restatement.[143]

Next, consider the customary allegation of a cyberattack class action complaint that the individuals whose personal

---

damages" as "items of damages for which a market exists and that therefore can be valued by reference to the market valuation").

143. Of course, just because such unauthorized access is not an actionable injury in common-law negligence does not mean such unauthorized access can never constitute actionable injury under some other tort theory, such as invasion of privacy. *See* Second Torts Restatement, *supra* note 69, § 652 (defining the contours of the tort of invasion of privacy). The question of the actionability of such unauthorized access under other tort theories is beyond the scope of this article. Similarly, the question whether such unauthorized access is an actionable injury in common-law negligence is an entirely different question from two other oft-debated questions in cybersecurity/privacy law, namely, whether such unauthorized access can constitute an "injury in fact" sufficient to sustain Article III standing or can constitute "substantial injury" sufficient to sustain an unfairness claim by the Federal Trade Commission ("FTC") under Section 5 of the FTC Act. Those two other questions are beyond the scope of this article but have been addressed by this author in two other recent articles. *See* Douglas H. Meal, *Booing Bohnak: How the Second Circuit Dropped the Article III Ball in Analyzing Standing in Class Actions Arising from Cyberattacks*, 16 CASE W. RES. J.L. TECH. & INTERNET 1, 16-23 (2025), also available at: https://scholarlycommons.law.case.edu/jolti/vol16/iss1/2 (hereinafter "Bohnak Article") (addressing whether unauthorized access can constitute an "injury in fact" sufficient to sustain Article III standing); Douglas H. Meal, *Misinterpreting Section 5(n) of the FTC Act: A Critique of the District Court's Decisions in* FTC v. Kochava, 43 J.L. & Comm. 1, 5-14 (2024), also available at: https://jlc.law.pitt.edu/ojs/jlc/article/view/296 (addressing whether unauthorized access to a consumer's personal information can constitute "substantial injury" sufficient to sustain an unfairness claim by the Federal Trade Commission ("FTC") under Section 5 of the FTC Act).

information was involved in the cyberattack suffered an "injury" actionable in negligence merely by reason of their being currently at risk of at some point in the future incurring an injury that would be actionable in negligence.[144] Insofar as such an allegation is predicated on the theory that the risk itself is an actionable injury, or that the risk caused the individuals to suffer an emotional harm, Section 47 expressly rejects these theories of an injury actionable in negligence.[145] And insofar as such an allegation is predicated on the theory that the individuals in question will need to incur out-of-pocket monitoring costs in the future to mitigate the risk, the Third Torts Restatement proposes to make such costs actionable in tort only where the risk is of serious bodily injury and only pursuant to a provision that the drafters recognize could justifiably be viewed as embodying an entirely separate tort and not merely a remedy for traditional torts like negligence.[146] As a result, an alleged "risk of future

144. *See, e.g.*, UnitedHealth Complaint, *supra* note 2, at Count I ("Negligence"), ¶ 413 (asserting that individuals whose personal information was stolen in the Change Health cyberattack thereby suffered "(10) a continued substantial and imminent risk of the misuse of their [p]ersonal [i]nformation," which "injury" is actionable in negligence).

145. *See* Physical/Emotional Harm Restatement, *supra* note 70, § 47, comment k (rejecting claims based on "fear of future injury," at least where serious bodily injury has not occurred and is not threatened); *accord*, Restatement (Third) of Torts: Miscellaneous Provisions (T.D. No. 3 2024) (hereinafter "Miscellaneous Provisions Restatement") Liability for Physical and Emotional Harm § __ (entitled "Medical Monitoring"), comment c.

146. *See* Miscellaneous Provisions Restatement, *supra* note 146, Liability for Physical and Emotional Harm § __ (entitled "Medical Monitoring") at subsection (1) and comment m. Whether the Third Torts Restatement should or will ultimately include such a theory of recovery based solely on an individual's risk of future injury is still being debated within the ALI and is subject to significant scholarly dispute. *See generally* Schwartz & Appel, *supra* note 82.

injury" from an cyberattack is likewise a claimed injury that never is in and of itself actionable in common-law negligence under the Third Torts Restatement.[147]

To be sure, a number of the non-economic injuries typically alleged in a cyberattack class action do meet the Third Tort Restatement's definition of "emotional harm," and thus are at least theoretically actionable in negligence under Section 47, because they are all at least "mildly unpleasant" and thus cause at least *some* "impairment or injury to a person's emotional tranquility."[148] Examples are alleged (1) emotional and mental distress and anguish resulting from the cyberattacker's access to, theft of, and/or posting of the personal information of the named plaintiff(s) and the putative class members; (2) disruption, by reason of the cyberattack, of the lives of the individuals whose personal information was involved in the cyberattack; and (3) those individuals' lost time and effort expended in responding to and preventing the threats and harm posed by the cyberattack, where such time and effort is not alleged to have caused them to suffer an out-of-pocket monetary loss and therefore did not give rise to economic harm.[149] But while these alleged

147. The question whether such a risk of future injury is an actionable injury in common-law negligence is an entirely different question from the question of whether such a risk can constitute an "injury in fact" sufficient to sustain Article III standing in a cyberattack class action. That Article III question is beyond the scope of this article but has been recently addressed by this author in a separate article. *See* Bohnak Article, *supra* note 144, at 24-35.

148. Physical/Emotional Harm Restatement, *supra* note 70, § 45 and § 45, comment a (defining "emotional harm" as an "impairment or injury to a person's emotional tranquility," and noting that the mental states encompassed by the term "emotional harm" include "all detrimental—from mildly unpleasant to disabling—mental conditions").

149. *See, e.g.*, UnitedHealth Complaint, *supra* note 2, at Count I ("Negligence"), ¶ 413 (asserting that individuals whose personal information was

injuries all meet the Third Tort Restatement's definition of "emotional harm," under the express wording of Section 47 emotional harm must be "serious" to be actionable in negligence.[150] A court seeking to apply the Third Torts Restatement to a negligence claim asserted in a cyberattack class action will accordingly need to decide whether the non-economic injuries typically alleged in such an action constitute not merely "emotional harm" but "serious emotional harm."[151]

The line between "serious" and "non-serious" emotional harm is, of course, not the brightest one imaginable given the inherent subjectivity of the word "serious." Happily, however, the ALI has provided the courts with considerable assistance in drawing that line in cyberattack class actions. For one thing, "there are [both] objective and subjective components to th[e] [serious emotional harm] requirement," such that "Section [47] applies only when the person seeking recovery has [in fact] suffered serious emotional harm" and, "[i]n addition, the actor's conduct [was] such that would cause a reasonable person to

---

stolen in the Change Health cyberattack thereby suffered "(5) lost value of their [p]ersonal [i]nformation; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their [p]ersonal [i]nformation; (7) disruption of their medical care and treatment; (8) disruption in obtaining pharmaceutical prescriptions; [and] (9) lost time [and] effort . . . responding to and preventing the threats and harm posed by the [cyberattack]," which "injuries" are actionable in negligence).

150. Physical/Emotional Harm Restatement, *supra* note 70, § 47 (limiting liability thereunder to a situation where an actor's "negligent conduct causes *serious* emotional harm to another") (emphasis added).

151. It will be for the court, not a jury, to decide whether the injuries alleged in such an action rise to the level of "serious emotional harm." *Id.* § 47, comment g (entitled "Role of judge and jury" and providing that "[d]etermination of which activities, undertakings, or relationships support recovery for stand-alone emotional harm is a matter of law for the court").

suffer serious emotional harm."[152] The objective component insures that Section 47 claims cannot survive a motion to dismiss merely because the plaintiff alleges that a cyberattack in fact caused him or her serious emotional harm. Further, the ALI explains that emotional harm cannot be found "serious" merely because it was a reasonably foreseeable consequence of the defendant's allegedly negligent conduct.[153] Section 47, the ALI points out, is intended to be "a general rule that negligently caused pure emotional harm is not recoverable even when it is foreseeable."[154] Thus, the ALI reasons, a reasonable foreseeability approach towards applying Section 47's serious emotional harm requirement "would eviscerate the general rule that pure emotional harm is normally not recoverable."[155]

---

152. *Id.* § 47, comment *l*. The subjective component of the serious emotional harm inquiry should make certification of a class impossible on a Section 47 theory of liability, as determination of liability would require a certification-defeating individualized inquiry of every class member as to whether he or she *in fact* suffered the serious emotional harm that a reasonable person allegedly would have suffered by reason of the cyberattack in question. *See supra* note 109. As a result, even if a cyberattack class action plaintiff could successfully plead a negligence claim under the Third Torts Restatement based on the emotional harm typically alleged in a cyberattack class action (which as discussed in text this author believes cannot be done), as courts begin to adopt the Third Torts Restatement's principles one would expect cyberattack class action plaintiffs to steer away from predicating their negligence claims on emotional harm, owing to the insuperable class certification problems created by doing so.

153. Physical/Emotional Harm Restatement, *supra* note 70, § 47, comment i ("Courts often state that the test for determining whether negligently caused emotional harm is recoverable is whether the actor reasonably should have foreseen the emotional harm. But foreseeability cannot appropriately be employed as the standard to limit liability for emotional harm.").

154. *Id*.

155. *Id.* § 48, comment g; *accord, id.* § 47, comment i ("[T]he rules stated in this Section and in § 48 are exceptions to a general rule that negligently

So how, then, are courts to determine if a plaintiff's alleged emotional harm by reason of a cyberattack is "serious" within the meaning of Section 47? On the one hand, emotional harm does not need to be so great that it rises to the level of "severe" within the meaning of Section 46 of the Physical/Emotional Harm Restatement, *i.e.*, in order to be "serious," emotional harm does not need to be distress "so severe that no reasonable [person] could be expected to endure it."[156] On the other hand, the Physical/Emotional Harm Restatement recognizes that "[c]omplete emotional tranquility is seldom attainable in this world, and some degree of emotional harm, even significant harm, is part of the price of living in a complex and interactive society."[157] "[T]he [serious harm] threshold for recovery under §§ 47 and 48 [thus] serves to . . . screen out modest or trivial harms that are endemic to modern society and therefore inappropriate for the legal system to address."[158] "The [serious harm] threshold reduces the universe of potential claims [under those provisions] by eliminating claims for routine, everyday distress that is a part of life in modern society."[159] By way of example, the ALI points out that "'mild anxiety that causes [a claimant] to recheck her work, but that only minimally interferes with her everyday

caused pure emotional harm is not recoverable even when it is foreseeable. Instead of relying on foreseeability to identify appropriate cases for recovery, the policy issues surrounding specific categories of undertakings, activities, and relationships must be examined to determine whether they merit inclusion among the exceptions to the general rule of no liability.").

156. *Id.* § 46, comment j (articulating standard for "severe" emotional harm under Section 46 of the Physical/Emotional Harm Restatement and explaining that "serious" emotional harm under Sections 47 and 48 is intended to be a lesser degree of harm than "severe").

157. *Id.* § 46, comment j.

158. *Id.* § 46, comment j.

159. *Id.* § 47, comment *l*.

life and for which she has not sought treatment' does not as a matter of law meet the requisite severity" of the serious harm threshold.[160] The Physical/Emotional Harm's test for "serious" emotional harm is thus analogous to its test for "serious" bodily injury in that both exclude harm that does not require medical treatment.[161]

Courts applying these guideposts to the emotional harms typically alleged in a cyberattack class action should have little difficulty in concluding that those harms do not rise to the level of "serious" for purposes of Section 47 and thus are not actionable in negligence under the Third Torts Restatement. Cyberattacks that target personal information are, unfortunately, so ubiquitous in our society that they have become a part of everyday life. Any distress or inconvenience or life disruption that occurs as a result of a cyberattack is thus a paradigmatic example of the "routine, everyday distress that is a part of life in modern society"[162] that Section 47's serious harm requirement screens out from liability as being "modest or trivial harms that are endemic to modern society and therefore inappropriate for the legal system to address."[163] Every American adult routinely has personal information of some sort involved in a cyberattack of some kind and, upon learning of such an event's occurrence,

---

160. *Id.* § 47, Reporter's Notes on comment *l* (quoting Lewis v. CITGO Petroleum Corp., 561 F.3d 698, 708-709 (7th Cir. 2009) ("Lewis")).

161. Physical/Emotional Harm Restatement, *supra* note 70, § 46, comment *l* ("Death, significant permanent disfigurement, or loss of a body part or function will almost always be sufficient for a jury to find th[e] [serious bodily injury requirement satisfied. By contrast, bruises, cuts, single simple fractures, and other injuries that do not require immediate medical treatment will rarely be sufficient to satisfy this requirement.")

162. *Id.* § 47, comment *l*.

163. *Id.* § 46, comment j.

routinely suffers some amount of distress or inconvenience or life disruption, even if it only amounts to the time expended in opening and throwing away the latest breach notification letter that has arrived in the mail. But such distress or inconvenience or life disruption "only minimally interferes with [one's] everyday life" and is not something for which one typically or reasonably would have "sought treatment."[164] As such, it is not "serious" emotional harm within the meaning of Section 47 and accordingly is not actionable in common-law negligence under the Third Torts Restatement.

c. No Activity, Undertaking, or Relationship Especially Likely to Cause Serious Emotional Harm

Section 47(b) expressly provides that serious emotional harm is actionable thereunder only where the actor's negligent conduct "occurs in the course of specified categories of activities, undertakings, or relationships in which negligent conduct is especially likely to cause serious emotional harm."[165] The ALI explains that this requirement cannot be satisfied by merely showing that the claimant was a "direct victim" of the actor's negligent conduct or that the serious emotional harm suffered by the claimant was a reasonably foreseeable consequence of that conduct.[166] Rather, the negligent conduct must have occurred when "an actor undertakes to perform specified obligations, engages in specified activities, or is in a specified relationship fraught with the risk of [serious] emotional harm."[167] The

164. *Id.* § 47, Reporter's Notes on comment *l* (quoting Lewis, *supra* note 101, 561 F.3d at 708-709).

165. Physical/Emotional Harm Restatement, *supra* note 70, § 47(b).

166. *Id.* § 47, comment f.

167. *Id.* § 47, comment b.

two leading examples of such specified obligations, activities, or relationships, per the ALI, are (1) delivering a telegram or other communication announcing death or illness and (2) handling a corpse or bodily remains, each of which specified activity is fraught with a risk of serious emotional harm being inflicted should the activity be negligently performed (say, by erroneously announcing the death or by mishandling the corpse).[168]

In the cyberattack class action context, however, even if serious emotional harm could theoretically result from a cyberattack (as discussed in Part II.B.2.b above this author thinks not), an entity's conduct in collecting the personal information that was involved in the attack, in performing an obligation to protect that information against a cyberattack, or in entering into the relationship pursuant to which the information was collected, would never be conduct "fraught" with the risk of inflicting such harm. Any entity that has human beings as employees, or as consumers of their product or service, necessarily collects and protects personal information from or about those human beings and accordingly is at risk of a cyberattack. But unlike an entity that delivers death announcements or handles corpses, negligence on the part of an entity that handles personal information does not regularly result in a cyberattack being successfully perpetrated against that entity, much less in serious emotional harm thereby predictably being inflicted on the individuals whose personal information was involved in the attack. Every entity in the world engages in the collection and protection of personal information, but only a tiny fraction of those entities have that information successfully cyberattacked in any given year, and only a tiny fraction of those successful attacks result in serious emotional harm to the individuals whose

168. *Id.* § 47, comment f.

information was involved (if, indeed, such attacks ever have that result, which this author disputes for the reasons discussed in Part II.B.2.b above). Accordingly, even assuming, contrary to the view taken in this article, that a cyberattack could on occasion result in serious emotional harm to one or more of the individuals whose information is involved in the attack, such harm would never be "especially likely to [be] caused"[169] by negligent conduct in the handling of personal information. As a result, such negligent conduct would never occur in the course of an activity, undertaking, or relationship that could qualify that conduct for liability under Section 47(b).

d. No Lack of Other Tort Coverage

As the ALI's comments on Section 47 point out, a "variety of other torts [*i.e.*, torts other than negligence] protect specific aspects of emotional tranquility."[170] Examples of such other torts "include defamation, invasion of privacy, false imprisonment, and malicious prosecution."[171] According to the ALI, "[t]he more general protection for emotional harm contained in [Section 47 of the Physical/Emotional Harm Restatement] should not be used to dilute or modify the requirements of those [other] torts."[172] Thus, "[w]hen torts exist that address more specifically protection of some specific aspect of emotional tranquility—such as one's concern about reputation or having one's private affairs revealed—liability should be left to the law developed

169. *Id.* § 47(b).

170. *Id.* § 47, comment o (entitled "Respecting the domain of other torts protecting specific emotional interests").

171. *Id.*

172. *Id.*

for those specific torts, and the rule provided in [Section 47] should not be applied to such conduct."[173]

The above-described further limitation on Section 47 liability for emotional harm is quite significant to how courts should apply the Third Torts Restatement to the non-economic harms typically alleged in a cyberattack. All of those alleged harms stem from "one's concern about . . . having one's private affairs revealed."[174] All of those alleged harms are, therefore, the sort of harm that is "address[ed] more specifically"[175] by the tort of invasion of privacy.[176] According to the ALI, then, liability for

---

173. *Id.* § 47, Reporter's Notes on comment o.

174. *Id*.

175. *Id*.

176. The ALI's project to develop the Third Torts Restatement's volume covering invasion of privacy, entitled *Defamation and Privacy*, was initiated in 2019 but there is no publicly available draft yet. *See* American Law Institute, *Projects, Restatement of the Law Third, Torts: Defamation and Privacy*, available at www.ali.org/project/torts-defamation-and-privacy. The ALI's most current restatement of the tort of invasion of privacy is therefore the one that appears in the Second Torts Restatement, *supra* note , at § 652 (defining the contours of the tort of invasion of privacy and its protection against injuries such an intrusion upon one's seclusion, *see id.* § 652B, and publicity being given to one's private life, *see id.* § 652D). In considering how Section 47's "69other torts" limitation applies to the non-economic harms typically alleged in a cyberattack class action, it matters not that the other tort in question (here, invasion of privacy) does not impose liability for some or all of those harms (as likely would be the case were Section 652 of the Second Torts Restatement applied to those harms). According to the ALI, Section 47 "should not be used to dilute or modify the requirements of th[e] [other] tort[]" in question. Physical/Emotional Harm Restatement, *supra* note 70, § 47(b), comment o. Thus, as long as a "tort[] exist[s] that address[es] more specifically protection of some specific aspect of emotional tranquility—such as [the tort of invasion of privacy addresses] one's concern about . . . having one's private affairs revealed—liability should be left to the law developed

conduct giving rise to the non-economic harms typically alleged in a cyberattack "should be left to the law developed for th[at] specific tort[], and the rule provided in [Section 47] should not be applied to such conduct."[177] For this further reason, courts applying the Third Torts Restatement to the non-economic harms typically alleged in a cyberattack class action complaint should find such harms inactionable in negligence as a matter of law.

III. CONCLUSION

As shown in Part I above, to date the U.S. courts have failed to come up with coherent or consistent answers to the question of what injuries typically alleged in a cyberattack class action should sustain a cause of action for common-law negligence based on the attack. As shown in Part II above, the Third Torts Restatement provides principles that the U.S. courts can use to answer that question consistently and coherently. As further shown in Part II above, under those principles the injuries typically alleged by the named plaintiff(s) in a cyberattack class action are not actionable in common-law negligence. Therefore, if the Third Torts Restatement gains widespread acceptance among the U.S. courts (as would be expected based on the widespread judicial acceptance of the ALI's other restatements and, in particular, of its prior torts restatements), negligence claims asserted in cyberattack class actions will at that point consistently be rejected by the U.S. courts for failure to allege an injury actionable in common-law negligence. As a result, individuals bringing such claims in cyberattack class actions will at that

---

for th[at] specific tort[], and the rule provided in [Section 47] should not be applied to such conduct." *Id.* § 47, Reporter's Notes on comment o.

177. Physical/Emotional Harm Restatement, *supra* note 70, § 47, Reporter's Notes on comment o.

point be left with whatever other common-law and statutory liability theories they may have to remedy the injuries they claim they and the putative class members incurred by reason of the cyberattack in question.

So is that outcome good, bad, or somewhere in between from a policy perspective? For the author of this article, that question is for the relevant policy makers (namely, the relevant state legislatures) to answer. And, indeed, some state legislatures have enacted statutes that create private rights of action in favor of individuals whose personal information is involved in a cyberattack,[178] while others have enacted affirmative defenses intended to protect entities that suffer cyberattacks against claims from individuals whose personal information was involved in a cyberattack.[179] But, again, at least in this author's

178. *See*, e.g., Cal. Civ. Code 1798.84(b) (providing that "[a]ny customer injured by a violation of [the reasonable security obligation set forth in Cal. Civ. Code 1798.81.5] may institute a civil action to recover damages"); Cal. Civ. Code 1798.150 (providing that a violation of the reasonable security obligation set forth in Cal. Civ. Code 1798.100(e) gives a consumer a private right of action if the violation results in unauthorized access to and exfiltration, theft, and disclosure of the consumer's "personal information" as defined in Cal. Civ. Code 1798.81.5).

179. *See, e.g.*, Tenn. Code 29-34-215 (providing that, where the specified statutory requirements are met, a private entity has no liability in a "class action lawsuit" resulting from a "cybersecurity event" unless the event was caused by willful and wanton misconduct or gross negligence on the part of the private entity); Iowa Code Title XIII, Chapter 554G (providing an affirmative defense to any tort cause of action brought under Iowa law or in Iowa courts alleging that a data breach involving personal information resulted from the defendant's failure to implement reasonable information security controls, if the defendant either satisfies all the requirements of Section 554G.2 or reasonably conforms to an industry-recognized cybersecurity framework); Ohio Rev. Stat. 1354.02(D)(1) (providing that a covered entity that satisfies Ohio Rev. Stat. 1354.02(A)(1), (B), and (C) "is entitled to an affirmative defense to any cause of action sounding in tort that is brought

view, that policy question should be decided *legislatively*. It emphatically *is not* a question for judges to decide by ignoring the established common-law principles they are bound to uphold in order to achieve an outcome that matches their personal policy preferences. As shown above, under established common-law principles as reflected in the Third Torts Restatement, the injuries typically alleged in a cyberattack class action are not actionable in common-law negligence. The U.S. courts should enforce those well-established principles and leave to the state legislatures, rather than taking it upon themselves, to decide whether different principles would be better as a policy matter.

---

under the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information); Utah Code 78B-4-702(1) (providing that "[a] person that creates, maintains, and reasonably complies with a written cybersecurity program that meets the requirements of [Utah Code 78B-4-702(4)], and is in place at the time of a breach of system security of the person, has an affirmative defense to a claim that (a) is brought under the laws of this state or in the courts of this state; and (b) alleges that the person failed to implement reasonable information security controls that resulted in the breach of system security"); Conn. Public Law 21-119 Section 1(b) (disallowing award of punitive damages "[i]n any cause of action founded in tort that is brought under the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable cybersecurity controls resulted in a data breach concerning personal information," where the defendant "created, maintained and complied with a written cybersecurity program that contains administrative, technical and physical safeguards for the protection of personal or restricted information and that conforms to an industry recognized cybersecurity framework, as described in subsection (c) of this section and that such covered entity designed its cybersecurity program in accordance with the provisions of subsection (d) of this section").

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

Author

The Sedona Conference

Contributing Editors

H. Christopher Boehning
Ross Gotler
Chuck Kellner
Kathleen Paisley
Chuck Ragan

Steering Committee Liaisons

Hon. James Francis (ret.)
Taylor Hoffman
Eric P. Mandel
Wayne Matus

Staff Editors

David Lumia
Craig Morgan
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, *Principles for International Arbitration*, 26 SEDONA CONF. J. 433 (2025).

PREFACE

Welcome to the August 2025 final version of The Sedona Conference's *Principles for International Arbitration* ("*Principles*"), 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 complex litigation, intellectual property rights, data security and privacy law, and artificial intelligence.

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 genesis of *Principles* dates to the spring of 2018, when the WG6 Steering Committee tasked a brainstorming group with considering (a) the applicability of *International Litigation Principles* to international arbitrations and associated data protection and cross-border discovery and disclosure issues, and (b) whether an appendix to *International Litigation Principles* or a stand-alone publication would be the correct approach. The brainstorming group ultimately concluded a stand-alone publication was warranted. The brainstorming group's proposal was the focus of dialogue of the WG6 Annual Meeting in St. Pete Beach, Florida, in January 2019. In the spring of 2019, the Steering Committee formed a drafting team to commence drafting *Principles*. The first draft of *Principles* was the subject of dialogue at a meeting of WG6 following the International Programme on Cross-Border Data Transfers and Data Protection Laws in Hong Kong in June 2019. A subsequent draft of *Principles* was the subject of dialogue at the WG6 Annual Meeting in New York in February 2020. The drafting team worked in earnest on refining *Principles* during the global COVID pandemic and presented the next iteration at the WG6 Annual Meeting in London

in January 2023. The draft was subsequently made available online to the public for review and comment before final publication.

The Sedona Conference thanks Contributing Editors Chris Boehning, Ross Gotler, Chuck Kellner, Kathleen Paisley, and Chuck Ragan for their contributions, and Judge James Francis, Taylor Hoffman, Eric Mandel, and Wayne Matus for their guidance and input as Steering Committee liaisons to the drafting team.

In addition to the work of the drafting team and the robust dialogue at the aforementioned WG6 meetings, 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 *Principles* that were circulated for feedback from the Working Group membership, and later to the public at large. On behalf of The Sedona Conference, I thank all of them for their contributions.

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, trade secrets, and artificial intelligence. 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.

Kenneth J. Withers
Executive Director
The Sedona Conference
August 2025

TABLE OF CONTENTS

PRINCIPLES FOR INTERNATIONAL ARBITRATION

Principle 1: During the course of an arbitration, Arbitral Participants should adopt a reasonable, cooperative, and proportionate approach to complying with all Data Protection Laws applicable to the proceedings while at the same time respecting the rights of the parties and their interests in the fair and efficient conduct of the proceedings.

Principle 2: The exchange of Documents and Evidence in International Arbitration should be minimized and narrowly tailored to the Documents and Evidence that are relevant to a party's claim or defense, nonduplicative, and material to the resolution of the matter. Disclosure should be undertaken in compliance with the Data Protection Laws as applied in a reasonable and proportionate manner, balancing the rights of the Data Subject and relevant third parties with those of the Arbitral Participants, reflecting the consensual nature of International Arbitration, and in consideration of the efficiency goal of the process (including cost and time), confidentiality, privacy, and enforceability.

Principle 3: An agreement between the parties as to the scope of document disclosure should be respected by an Arbitral Tribunal,

provided their agreement is consistent with Principles 1 and 2.

Principle 4: Where document disclosure is considered appropriate, and the parties are not able to agree on the scope of the disclosure, or if the agreement they propose is inconsistent with Principles 1 or 2, the Arbitral Tribunal should apply Principles 1 and 2 in deciding the extent of disclosure to be ordered.

Principle 5: Applying Data Protection Laws to arbitration proceedings may require the Arbitral Tribunal to issue binding Data Protection Directions on the parties applicable to the Data Protection Laws at issue. The Arbitral Tribunal should consider issuing such directions after judging the parties' conduct under a standard of good faith, reasonableness, and proportionality, taking into account the considerations in Principles 1–4. While not binding on them, courts and Data Protection Authorities should respect and give reasonable deference to the decisions of the Arbitral Tribunal[1] as to the application of Data Protection Laws to the

1. Here, Arbitral Tribunal refers to the panel in its decision-making capacity (please see the formal definition of the term "Arbitral Tribunal" in Section II, *infra*). We note, however, that the arbitral institutions may establish rules and controls impacting privacy interests and should be guided by these principles as well.

Processing of Protected Data in International Arbitrations.

Principle 6: Arbitral Participants should put in place technical and organizational measures appropriate to ensure a reasonable level of information security of the Documents and Evidence, taking into account the scope and risk of the Processing, the capabilities and regulatory requirements of the Arbitral Participants, the costs of implementation, and the nature of the information being processed or transferred, including whether it includes Protected Data, privileged information, or sensitive commercial, proprietary, or confidential information.

I. INTRODUCTION

The Sedona Conference launched its Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6) in July 2005 with a program in Cambridge, England, entitled *International Issues: E-Information Management, Disclosure and Discovery*. In the ensuing years, WG6 has produced more than a dozen publications in furtherance of its mission "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." One significant area of dispute resolution that has not been addressed in those papers is discovery and disclosure in international arbitration. This publication seeks to fill that gap.

International commercial arbitration is a consensual process pursuant to which persons and commercial entities agree that disputes arising out of or relating to their business relationship should be subject to arbitration and exclude or severely limit court jurisdiction. These entities may choose arbitration for a variety of reasons, including certain characteristics of international arbitration that are discussed in Section III of this paper. Two of those features that are important are that arbitration: (1) may be private and (2) is intended to be a more efficient than litigation for resolving disputes.

Because arbitration is a matter of contract, participants are not bound to follow a defined set of rules or procedures, as is generally the case in litigation, but have substantial flexibility to tailor the dispute resolution proceedings—including the law, language, and procedural rules to be applied—to fit the particularities of their matter. However, these issues can also be addressed in the arbitration agreement, which then becomes binding on the parties unless they agree otherwise.

Fact-finding is an essential element of International Arbitration, as in all forms of dispute resolution. Given the global nature of commerce, the fact-finding process in arbitration often implicates the cross-border processing of significant amounts of data. Such data may include Personal or other Protected Data subject to various data protection laws and regulations in jurisdictions throughout the world.

With this background in mind, WG6 offers the *Principles for International Arbitration* ("*Principles*") relating to the secure processing, review, and disclosure of data—particularly Personal or other Protected Data—in the specific context of document disclosure in International Arbitration. The purpose of *Principles* is to suggest a reasonable and proportional approach to the use and protection of data in international arbitration that: (1) respects the data protection and privacy rights of relevant Data Subjects while at the same time recognizing the due process rights of the Arbitral Participants, including the right of parties to adduce evidence material to resolution of the matter and (2) ensures reasonable and good-faith compliance with Data Protection Laws, while at the same time respecting the quasi-judicial role of International Arbitration and ensuring that arbitral proceedings are not unduly hindered.

The focus of *Principles* is on the cross-border data transfer aspects of International Arbitration. By adopting the suggested approach and striking the appropriate balance, participants in International Arbitration can mitigate potential conflicts with privacy laws and regulations in the context of cross-border data transfers during International Arbitration Proceedings.

A. Structure of This Publication

Principles starts with a statement of the six Principles of International Arbitration, followed by this Introduction (Section I) and a list of Definitions (Section II). Section III provides

background on the characteristics of international commercial arbitration. The core of the paper can be found in Section IV, which addresses the six Principles of International Arbitration and provides commentary for each principle with explanatory guidance. A conclusion follows in Section V.

B. Intended Audience

Principles is primarily addressed to the parties to the arbitration, their legal counsel, the Arbitral Tribunal, any arbitral institution administering the dispute, and any consultants, advisors, or experts retained during the arbitration (collectively "Arbitral Participants," as defined in the Definitions section below).

Principles is additionally addressed to data protection authorities and other enforcement bodies responsible for applying Data Protection Laws throughout the world. Given the important role that arbitration plays in the cross-border administration of justice, it is hoped that supervisory authorities will find *Principles* to be a valuable resource in assessing whether the Arbitral Participants have adequately addressed the rights of Data Subjects and applied data protection principles in their arbitration proceedings.

Principles advances the position that data protection and data disclosure can co-exist in International Arbitration. Data Protection Laws are not antithetical to the core tenets of International Arbitration addressed herein. For example, Arbitral Participants regularly come to agreements to ensure that data processed, disclosed, transferred, and maintained in their arbitration will be subject to rigorous security and confidentiality requirements geared towards compliance with Data Protection Laws. In the same vein, Arbitral Participants often make efforts to minimize disclosure where possible in line with international data minimization principles.

C. *Role of Cooperation in International Arbitration*

Principles is based on the belief that, through cooperation, Arbitral Participants and Data Protection Authorities can work together to ensure that the rights and needs of both Data Subjects and Arbitral Participants are considered and met. Such cooperation is a hallmark of The Sedona Conference, as reflected in its widely accepted *Cooperation Proclamation*, published in July 2008,[2] as well as in the subsequent publication, *The Case for Cooperation*.[3]

Accordingly, *Principles* is intended to facilitate the process of cooperation among the Arbitral Participants, and to help chart the course for compliant, efficient, and defensible data processing, review, and disclosure of data in international commercial arbitration proceedings. In doing so, *Principles* is intended to promote and advance the complementary interests of fair adjudication and data protection.[4]

---

2. The Sedona Conference, *Cooperation Proclamation* (2008), 10 SEDONA CONF. J. 331 (2009 Supp.), *available at* https://thesedonaconference.org/publication/The_Sedona_Conference_Cooperation_Proclamation (calling upon adversaries to work collaboratively during the discovery phase of litigation as a means of reducing costs and delays). These tenets can and should also be applied in the context of International Arbitration.

3. The Sedona Conference, *The Case for Cooperation*, 10 SEDONA CONF. J 339, 344 (2009 Supp.) (observing that "cooperation is not in conflict with the concept of zealous advocacy. Cooperation is not capitulation.").

4. While the *Principles for International Arbitration* ("*Principles*") is principally intended to guide Arbitral Participants partaking in international commercial arbitration, it is anticipated that it also will be a valuable resource to parties in bilateral investment treaty arbitration, mediation procedures, and other related contexts, including arbitrations between parties from a single country for which cross-border transfers of personal information may be necessary or appropriate.

D. Rejecting the Weaponization of Data Protection Laws

Some aspects of *Principles* are worth highlighting at the outset. First, Arbitral Participants and Data Protection Authorities should take care to ensure that Data Protection Laws are not used as a shield to prevent the disclosure of key information in the course of an International Arbitration. Rather, when data-related disputes arise, *Principles* urges that Arbitral Participants work together in good faith to find practical solutions based on the reasonable and proportional needs of the individuals involved, ensuring that the rights of Data Subjects are respected, and that material information is not withheld from the Arbitral Tribunal so as to impair its ability to fairly adjudicate the matter. Key considerations in doing so may include: (1) the risk to the Data Subject were the data to be processed and disclosed; (2) the hardship on the Arbitral Participants were the data to be withheld; (3) the categories and scope of the data at issue, including whether it contains Personal Data, "special or sensitive category" data, or criminal offense data; and (4) the protections in place and mitigating measures available to ensure the data will be kept secure and confidential, preventing further processing or onward transfer.

II. DEFINITIONS

The following definitions apply throughout the *Principles for International Arbitration*:

"**Arbitral Participants**" means the parties to the arbitration, their legal counsel, the Arbitral Tribunal, any arbitral institution administering the dispute, and any consultants, advisors, or experts retained during the arbitration.

"**Arbitral Tribunal**" means the panel of adjudicators (arbitrators) convened to hear and resolve a dispute submitted for International Arbitration. The Arbitrational Tribunal is distinguished from the arbitral institution (e.g., ICC, LCIA, JAMS, ICDR, AAA, and CPR).[5]

"**Data Controller**" means the natural or legal person, public authority, agency, or other body that alone or jointly with others determines the purposes and means for the processing, transfer, and disclosure of Protected Data. For the purposes of *Principles*, it is assumed that Arbitral Participants are Data Controllers or joint controllers for at least some of these activities during International Arbitration proceedings.

"**Data Protection Authorities**" means any person or entity charged with enforcing Data Protection Laws.

"**Data Protection Directions**" are procedural directions issued by an Arbitral Tribunal in the form of a procedural order, terms of reference, or a data protection protocol setting out how data protection will be addressed during the arbitration. They

5. ICC is formally known as the International Chamber of Commerce, International Court of Arbitration; LCIA is the London Court of International Arbitration; the arbitral institution "JAMS" was originally named Judicial Arbitration and Mediation Services; ICDR is the International Centre for Dispute Resolution—the international division of the American Arbitration Association (AAA); CPR refers to the International Institute for Conflict Prevention & Resolution.

may be issued on an agreed basis or ordered by the Arbitral Tribunal.

"**Data Protection Laws**" means any law or regulation—regardless of whether it takes the form of a Data Protection Law, a privacy regulation, a blocking statute, or other protection—that addresses the processing of Personal Data, including appropriate usage, transfer, or disclosure of data; requires safeguarding data; or imposes obligations in the event of compromises to the security or confidentiality of data.

"**Data Subject**" means any person or entity whose Protected Data is or may be processed, transferred, or otherwise disclosed.

"**Documents and Evidence**" means documents, electronically stored information ("ESI"), and any other relevant evidence that may be exchanged during an International Arbitration (as defined below).

"**International Arbitration**" means an arbitration procedure whereby the parties to a cross-border dispute agree either by contract or another legally binding mechanism to submit disputes that may arise between them to an Arbitral Tribunal for decision.

"**Personal Data**" means any data that reasonably relates, directly or indirectly, to an identified or identifiable natural person.

"**Processing**" includes any operation, activity, use, or application performed upon Protected Data by automatic or other means, such as, for example, alteration, collection, disclosure, processing, recording, storage, retrieval, transfer, or use.

"**Protected Data**" is any data irrespective of its form (e.g., paper, electronically stored information, images, etc.) that is subject to Data Protection Laws, including, but not limited to, Personal Data.

III. CHARACTERISTICS OF INTERNATIONAL ARBITRATION

This section is included for the benefit of Arbitral Participants who may be new to International Arbitration and to explain the context from which *Principles* emerges. This section serves as background only, and readers are also referred to the ICCA-IBA Roadmap on Data Protection in International Arbitration,[6] and to the ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration.[7]

International Arbitration is a method of dispute resolution that is often chosen as an alternative to resolving a dispute in court. This includes both:

- commercial disputes, where the parties are engaged in commercial activities and agree that any disputes arising from those commercial activities will be subject to arbitration; and
- investor-state disputes, where an investor brings a claim pursuant to a treaty—these claims are often, but not always, administered by international organizations.[8]

---

6. International Council for Commercial Arbitration ("ICCA"), The ICCA Reports No. 7: The ICCA-IBA Roadmap to Data Protection in International Arbitration (2022), *available at:* https://www.arbitration-icca.org/icca-reports-no-7-icca-iba-roadmap-data-protection-international-arbitration.

7. ICCA, THE ICCA REPORTS NO. 6: ICCA-NYC BAR-CPR PROTOCOL ON CYBERSECURITY IN INTERNATIONAL ARBITRATION (2022), *available at:* https://www.arbitration-icca.org/icca-reports-no-6-icca-nyc-bar-cpr-protocol-cybersecurity-international-arbitration. ICCA is an acronym for the International Council for Commercial Arbitration; NYC references the New York City Bar Association; and CPR refers to the International Institute for Conflict Prevention and Resolution.

8. Different legal instruments may have different definitions of an international organization. Pursuant to the European Union's General Data Protection Regulation ("GDPR") Art. 4(26), "international organization" means an organization and its subordinate bodies governed by public international

Important features of International Arbitration are:

- the centrality of consent, in that parties must have agreed to resolve the dispute by arbitration (in the case of investor-state arbitration, this consent is found in a treaty);
- the importance of due process to the enforceability of awards;
- its neutrality and flexibility, since the parties to commercial disputes can choose the law under which to resolve the dispute, the language in which to conduct the proceedings, and the procedural rules to be applied during the proceedings that are typically selected in the arbitration agreement and become binding on the parties unless amended (in the case of investor-state arbitration, this freedom is circumscribed by the treaty);
- an emphasis on party autonomy, including the ability to tailor the proceedings to fit the particularities of the case (in the case of investor-state arbitration, this autonomy is circumscribed by the treaty);
- depending on the arbitration agreement, party autonomy often allows party participation in the selection of the arbitrator(s) with experience or expertise appropriate to the dispute;
- the ability to conduct private and often confidential proceedings in commercial disputes and to limit the disclosure of Personal and Protected Data in the award (in some cases investor-state

law, or any other body that is set up by, or on the basis of, an agreement between two or more countries.

arbitrations are resolved with some degree of transparency to the public);

- the importance of efficiency;
- the parties' fundamental right to present and prove their respective cases, which includes gathering and producing evidence, and in certain instances obtaining evidence from other parties; and
- fair and equitable treatment of the parties.

A. Type of Arbitration Proceedings

As noted above, *Principles* addresses two types of International Arbitration proceedings (i.e., commercial and investor-state). The type of arbitration, however, does not determine whether Data Protection Laws apply. That issue is determined by whether the data Processing falls within the material and jurisdictional scope of the relevant laws. *Principles,* therefore, does not distinguish between international commercial and investor-state arbitrations; also, *Principles* may be applied to other types of International Arbitration as appropriate, even though not specifically called out within.

1. Commercial Arbitration

Consent is fundamental to arbitration. International commercial arbitration is undertaken pursuant to the agreement of the parties. The parties may include an agreement to arbitrate in their business contract or enter into a separate agreement after a dispute arises. In either event, the agreement may refer to a set of arbitration rules, in which case those rules will govern the proceeding. Generally, proceedings take place before a tribunal made up of a sole arbitrator or a panel of three arbitrators.

In applying Data Protection Laws to arbitration, it will be important to recall that the Arbitral Participants are all required

to comply with the arbitration agreement, including any arbitration rules referred to therein, provided that in doing so, they comply with mandatory principles of law, including Data Protection Laws.

2. Investor-State (or Treaty) Arbitration

International Arbitration may be carried out on the basis of an agreement to arbitrate contained in a treaty rather than a contract between two commercial entities. A dispute arising under a treaty may, for example, be between an investor and a state, or between two states.

While investor-state arbitration is conducted on a different legal basis than commercial arbitration, this does not, in principle, alter the way that Data Protection Laws apply to the Arbitral Participants unless this is expressly provided for in the Data Protection Law.

However, when the dispute is administered by an international organization, which is often the case in investor-state arbitration, the Data Protection Laws may exclude international organizations from its scope. Furthermore, the host country agreement and the privileges and immunities of the international organization in question generally contain special rules, pursuant to which the international organization itself, and potentially others, may be immune from or fall outside the scope of the otherwise applicable Data Protection Laws.

This must be determined on a case-by-case basis and for each Arbitral Participant individually. Moreover, even when Data Protection Laws do not apply, the international organization may have its own data protection policy.

B. Ad Hoc versus Administered Arbitration

International commercial or treaty arbitration may be conducted under the auspices of an arbitral institution or

international organization or on an ad hoc basis without any administering institution, although even ad hoc arbitrations may use an arbitral institution or international organization to hold funds or assist with the appointment of arbitrators.

It is more common for arbitrations to be administered, which implies that an arbitral institution or international organization provides administrative support and some degree of oversight and review of awards. The extent of oversight and review varies greatly among institutions and international organizations. Moreover, some institutions provide secure online data platforms to facilitate the exchange of information during the arbitration process.

C. Enforceability

One of the main benefits of International Arbitration is that, unlike judgments of national courts in matters involving parties from different nation-states, International Arbitration awards are widely enforceable under international treaties, most notably the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the "New York Convention") and the Washington Convention on the Settlement of Investment Disputes between States and Nationals of Other States (the "Washington Convention").

The New York Convention is an international treaty providing that the contracting states will enforce arbitration awards rendered in other contracting states unless the award runs afoul of one of the few listed bases for the refusal of enforcement. Bases for the refusal of enforcement focus on the agreement to arbitrate and the arbitrability of the subject matter, and enforcement can be denied if the award has been set aside at the arbitral seat (with some exceptions) or if enforcement would otherwise be contrary to the public policy of the enforcing state. This latter basis is often used to argue that awards resulting from

proceedings that lacked due process or violated the right to be heard or to apply fair and equitable treatment to the parties should not be enforced, although in practice these arguments are rarely successful in overturning an arbitral award. At the time of publication, 172 states were parties to the New York Convention,[9] which makes the enforcement of awards under its terms essential to the fabric of International Arbitration.

The Washington Convention also provides an enforcement mechanism for investor-state awards issued under the Washington Convention. International Centre for Settlement of Investment Disputes (ICSID) awards are "automatically" enforceable as a judgment of the national courts in any contracting state, unless annulled in accordance with the procedure set forth in the Washington Convention. The bases for annulment are even narrower than those set forth in the New York Convention.

D. Applicable Law

In any given arbitration, different legal regimes may be applicable or relevant to different aspects of the case. By way of example, in the context of a hypothetical International Arbitration:

- the governing law of the contract underlying the parties' dispute may be English law;
- the legal seat of the arbitration may be Geneva, bringing in the application of Swiss law to certain procedural aspects of the arbitration;
- the parties to the arbitration may be established in the U.S. and in Brazil, with regulatory and other reporting requirements under the relevant local laws;

9. *Contracting States*, NEW YORK CONVENTION, https://www.newyorkconvention.org/contracting-states (last visited Dec. 19, 2024).

- the parties' legal counsel will be subject to both legal and professional obligations (including regarding privilege) in the jurisdiction(s) where they are admitted to practice;
- the Arbitral Participants are all required to comply with applicable economic sanctions and money-laundering laws and regulations; and
- the Arbitral Participants are all required to comply with the Data Protection Laws and regulations applicable to them.

All of these legal regimes constrain the behavior of the Arbitral Participants. In particular, the law of the legal seat of the arbitration places procedural constraints on the proceedings and the arbitrators. If the law at the legal seat is not respected, the award is at risk of being vacated or refused enforcement under the New York Convention.

As demonstrated by the above hypothetical, data protection is just one of several applicable laws to be taken into account by Arbitral Participants. As with compliance with sanctions and money laundering regulations, compliance with Data Protection Laws is mandatory and part of the legal landscape in which arbitrations are being conducted.

Most Data Protection Laws do not expressly address their application to arbitration. That is why it is important to think through and document the solutions adopted within the framework of whatever Data Protection Laws apply to a given proceeding, in order to (1) demonstrate compliance efforts if challenged, (2) defend the Arbitral Participants' good-faith efforts in the event of an unintended data protection breach or cybersecurity incident, and (3) minimize disruption to the proceeding by anticipating and resolving issues early on and ensuring agreement on those solutions among Arbitral Participants.

E. Conduct of Proceedings

International Arbitrations are conducted according to procedures and principles drawn from a mix of legal traditions, of both common law and civil law backgrounds. However, notwithstanding the diversity of the Arbitral Participants and the laws and procedures under which they may be conducted, international commercial arbitral proceedings have developed a certain level of uniformity in recent years.

The arbitration usually begins with a demand or request for arbitration. If the arbitration agreement provides for an arbitral institution, that institution and its rules typically govern the submission of additional preliminary pleadings and appointment of arbitrators.

One of the commonalities in International Arbitration that has developed in recent years is an early meeting of the Arbitral Participants to specify the procedure and timeline to be applied during the proceedings, including how evidence is adduced.

The Processing of evidence in an International Arbitration typically starts with the parties, who, before lodging a claim, will typically gather the facts and the evidence supporting those facts. This evidence is then transferred to their legal counsel, who will determine which of those facts and evidence to present to a tribunal in support of their party's case.

Proceedings often include a "disclosure" process, in which each party may request documents from the other(s) that are relevant to their own case and material to resolution of the matter, following which disclosure may take place voluntarily or as ordered by the tribunal. Following disclosure, a more limited group of further evidence may be submitted by each party to the tribunal as proof of its case.

As information submitted in an International Arbitration will often contain Protected Data, the gathering, Processing, production, and adducing of evidence needs to be squared with

the rights of the Data Subjects who are identified in or are identifiable through the evidence, while at the same time recognizing the due process rights of the parties to the disputes. Parties should also consider that the arbitration award itself may contain Protected Data. These principles must be reconciled in a manner that is reasonable and proportionate to the rights at issue.

It is a general principle of arbitration that each party has the burden of proving its claims in the manner that it sees fit, within the applicable arbitration agreement and the law and under the control of the Arbitral Tribunal. In presenting its case, a party will typically submit written, and in many cases oral, evidence in support of it. That evidence may take many forms, such as written statements by a witness of fact, the opinion of an expert, or written evidence including business documents, correspondence, emails, images, or video. In its award, the Arbitral Tribunal decides whether each party has discharged its burden of proof in relation to the allegations made.

The documentary and other evidence exchanged in International Arbitration proceedings will typically exceed that which would be exchanged in typical civil law or Islamic (Sharia) court proceedings, but it may be less than that exchanged in common law courts, particularly in the United States under broad rules of civil procedure for discovery. This middle ground between the various legal systems reflects that International Arbitration involves parties from different legal traditions who have chosen arbitration over public, civil litigation as an arguably more efficient dispute resolution method.

F. Due Process, Fair and Equitable Treatment, and the Right to be Heard

Due process is the all-encompassing obligation of a tribunal to ensure procedural fairness. Due process requirements are

enshrined in most, if not all, modern legal systems, arbitration rules, national arbitration laws, and the New York Convention.

An important due process requirement is affording all parties to the arbitration an opportunity to present their case, also referred to as the "right to be heard." This includes giving the parties notice of and access to the same information about the proceedings, the opportunity to and reasonable time in which to make submissions of evidence and legal arguments, and allowing them the opportunity to respond to the submissions of the other party(ies). The right to be heard generally encompasses a party's right to be represented by the legal counsel of its choice and to be heard by an independent and impartial tribunal. Moreover, the tribunal's decision cannot be based on grounds that the parties did not have an opportunity to address.

Another component of due process is the right to fair and equitable treatment. Many arbitration rules and national arbitration laws explicitly require that parties to an arbitration be treated equitably, and it is crucial in International Arbitration that no party has an unfair advantage.

Where legally allowed, these fundamental due process rights of the parties may be considered in deciding how the Data Protection Laws are to be applied to Arbitral Participants in International Arbitration proceedings, provided that the rights of Data Subjects are adequately protected. Due process, fair and equitable treatment, and the right to be heard require a tribunal to enable the parties to present their cases and the evidence supporting them. At the same time, Arbitral Participants must respect and comply with applicable Data Protection Laws ensuring that the rights of Data Subjects are protected.

G. Party Autonomy

The principle of party autonomy is an important reason parties opt for arbitration, as it allows them to tailor the proceedings

to the particularities of the dispute and the needs of the parties. Under this principle, parties enjoy a considerable degree of freedom to agree as to how the arbitral process should be structured and conducted. Indeed, under the New York Convention an arbitral award may be denied recognition if the proceedings that led to the award were conducted in a manner that is not in accordance with the parties' agreement.

Where parties do not agree on matters related to the conduct of proceedings, the Arbitral Tribunal generally has broad discretion in deciding those issues. In addition, party autonomy may be limited by mandatory provisions of the law of the legal seat of the arbitration. Failure to comply with such provisions may result in setting aside the award and/or refusal of enforcement. Such mandatory rules often include the fundamental principles of due process, fair and equitable treatment, and the right to be heard, described above. Moreover, party autonomy is restricted by mandatory principles of the substantive law applicable to the arbitration, which will often include Data Protection Laws.

H. Procedural Efficiency

The efficiency of arbitral proceedings over litigation may be one reason to choose International Arbitration; it is an effort to avoid unnecessary procedures and costs that come with standard litigation in public courts. Accordingly, the arbitrators should consider procedures that will not cause undue delay or create unnecessary complexity. Data Protection Laws should be applied in this context to International Arbitration, while protecting the rights of Data Subjects impacted by the proceeding. Unless properly managed, the strict application of some of the principles of Data Protection Law could lead to a significant expenditure of time and resources. Data protection principles incorporated into applicable Data Protection Laws should

therefore be applied reasonably and proportionately, having due regard for the efficiency of the proceedings.

I. Privacy and Confidentiality

International Arbitration proceedings are not accessible to the public or third parties, reducing the probability of public disclosure of Protected Data.[10] However, in limited situations, information disclosed in a proceeding and, especially arbitration awards, may be further disclosed. Due to the consensual nature of commercial arbitration, the parties can agree that strict confidentiality obligations will apply to everyone involved in the proceedings. Where agreement is not possible, the Tribunal can issue a protective order. The consideration of protective orders is encouraged to address these situations and may be able to reduce the risk of disclosure of Protected Data. Privacy and confidentiality are often highly valued by commercial parties, who may not wish their disputes to be heard in an open, publicly accessible courtroom because of commercially sensitive information (e.g., trade secrets and cost/pricing information), the wish to limit damage (e.g., reputational), and the desire to enhance the efficient resolution of the dispute.

In the context of commercial arbitration, the award may be intended to remain confidential. Even in confidential arbitrations, however, there is a risk that the award will become public if it is enforced in a country where awards (or parts thereof) become public in the enforcement process. Furthermore, arbitral institutions increasingly publish awards and other decisions (or excerpts thereof) as a matter of course, unless the parties object.

In the context of investor-state arbitration, given the involvement of state actors, case materials such as pleadings,

10. Investor-state arbitrations are typically public, and thus a noted exception.

submissions, procedural orders, decisions, and awards are often published. This is because in treaty arbitration, there generally is a greater desire for transparency, especially where public interests are at stake.

It is foreseeable in international commercial or investor-state arbitrations that, as with some courts, public access to proceedings and published materials may unavoidably expose some Personal Data. Depending on the obligations of the Arbitral Participants under the applicable Data Protection Law, it may, therefore. be necessary for the Arbitral Tribunal or the arbitral institution to require proactive measures to protect that Personal Data in filings (e.g., by means of redaction).

IV. PRINCIPLES OF INTERNATIONAL ARBITRATION AND COMMENTARIES

Principle 1: During the course of an arbitration, Arbitral Participants should adopt a reasonable, cooperative, and proportionate approach to complying with all Data Protection Laws applicable to their proceedings, while at the same time respecting the rights of the parties and their interests in the efficient conduct of the proceedings.

Comment

Principle 1 recognizes that tension can exist between disclosure in International Arbitration and Data Protection Laws. Arbitral Participants should be aware of obligations triggered by applicable Data Protection Laws and should apply them in a reasonable and proportionate manner that respects the rights of Data Subjects and third parties while at the same time respecting the rights of the Arbitral Participants, the integrity of the proceedings, and the need for the proper, prompt, and efficient administration of justice through arbitration.

The Arbitral Participants should consider compliance with Data Protection Laws that are applicable to the proceedings or to any Data Subjects at issue in their proceedings—as well as compliance obligations under those Data Protection Laws, which are usually of mandatory application and apply alongside the applicable arbitration rules to both international commercial and investor-state arbitrations. Such consideration should take place no later than the organizational meeting conducted early in the arbitration to establish the procedural guidelines and timetable for the proceedings in order to ensure compliance.

When balancing compliance with Data Protection Laws with the parties' due process and efficiency interests, Principle 1 encourages the Arbitral Participants to consider, among other things:

A. the scale, extent, and nature of the Personal Data, "special category" data, data relating to a child, or criminal offense data being Processed and the lawful basis for the Processing;

B. the degree of risk to the rights and interests of Data Subjects from the Processing of their Personal Data, taking into account the extent to which various privacy, confidentiality, and security protections and mitigating measures have been put in place to anonymize, secure, or otherwise limit this risk and the extent to which the Data Subjects have been notified of and given an opportunity to challenge the Processing;

C. the potential impact on the rights and interests of the parties to the International Arbitration and third parties were the data to be withheld, taking into account whether the information sought via disclosure could be obtained through other, less invasive means;

D. whether cross-border transfers will be required for the orderly conduct of the proceedings and whether measures have been, or may be, taken to provide a lawful basis for any such transfers (for example, Standard Contractual Clauses under the EU General Data Protection Regulation ("GDPR")); and

E. the protections in place to ensure that the data is and will be kept secure and confidential throughout the arbitral proceedings, and whether any other mitigating measures, such as redaction or pseudonymization of Personal Data, could be put in place to enhance such protections.

Principle 2: The exchange of Documents and Evidence in International Arbitration should be minimized and narrowly tailored to the Documents and Evidence that are relevant to a party's claim or defense, nonduplicative, and material to the resolution of the matter. Disclosure should be undertaken in compliance with the Data Protection Laws as applied in a reasonable and proportionate manner, balancing the rights of the Data Subject and relevant third parties with those of the Arbitral Participants, reflecting the consensual nature of International Arbitration, and in consideration of the efficiency goal of the process (including cost and time), confidentiality, privacy, and enforceability.

Comment

Arbitration is a means to resolve disputes different from and as an alternative to litigation. For common law countries, one difference between arbitration and litigation is that prehearing discovery or disclosure of information is generally more limited in scope in arbitration. In International Arbitration, prehearing disclosure of information is even more limited, in part because some participants come from countries where no prehearing disclosure occurs; indeed, some arbitral rules discourage prehearing disclosure requests.

The following recommendations are designed to further the objectives embodied in Principle 2:

A. International Arbitration is undertaken by contracting parties or those that are subject to treaty rights seeking to reach a resolution that is fair

and equitable, in accordance with applicable law, and can be enforced globally under applicable law and international treaties. Where possible, it is, and should be, a substantially cooperative endeavor.

B. International Arbitration should be cost effective and time efficient. Core issues are, and should be, quickly identified and evaluated. Arbitral Participants should not waste resources on ancillary issues.

C. Personal Data should not be subject to unnecessary Processing, disclosure, or transfer, especially when it contains Protected Data.

D. International Arbitration is private and can be made substantially confidential. Where confidentiality attaches, the privacy of the Arbitral Participants is, and should be, recognized and respected. This may be mandated when the International Arbitration is subject to the Data Protection Laws.

A significant obstacle to the achievement of these benefits occurs where expansive disclosure of Documents and Evidence of possible relevance to the disputes is permitted without sufficient justification under Principles 1 and 2. With the proliferation of electronic communications in recent years, the extent of available Documents and Evidence (especially ESI) has grown exponentially, as have party disagreements related to their collection and exchange. Compounding this problem, the rules and practice governing the exchange of Documents and Evidence—including the Data Protection Laws applicable to such exchange—vary widely across jurisdictions throughout the world.

Moreover, tension may exist between the private nature of arbitrations and the transparency requirements to Data Subjects under some Data Protection Laws. Parties, especially those who frequently are part of International Arbitration, may consider addressing this through ensuring that the applicable privacy notices or processes include appropriate references to the potential use of Protected Data in such proceedings.

Acknowledging these obstacles, Principle 2 encourages parties to work together in International Arbitration to scope the exchange of Documents and Evidence to that which is nonduplicative, relevant, material to resolution of the dispute, and proportional to the needs of the matter. In doing so, Principle 2 recognizes two fundamental tenets governing the exchange of Documents and Evidence in International Arbitrations:

A. The Documents and Evidence Processed in International Arbitrations, including any Protected Data contained therein, should be minimized.

   1. Parties should engage in targeted collection efforts, and to the extent feasible should collect and exchange only unique and nonduplicative Documents and Evidence that are relevant and material to the resolution of the dispute.

   2. To the extent that parties must collect and exchange Protected Data, such data should be limited to that which is proportional to the needs of the dispute and that which is necessary and cannot be obtained from other sources.

B. To the extent available and consistent with the efficiency goal of the process (including cost and

time), the Arbitral Participants are encouraged to leverage technology solutions during the proceedings, including for the disclosure and management of Documents and Evidence, where applicable.

1. Technology solutions may facilitate compliance with Data Protection Laws during the International Arbitration by minimizing the scale of Documents and Evidence to be collected and exchanged, enabling pseudonymization or redaction of Protected Data where possible, tracking and minimizing cross-border transfers of Protected Data, securing Documents and Evidence including Protected Data on secure servers with advanced data security infrastructures, and ensuring timely destruction of Documents and Evidence.

2. Assuming access to such solutions is equally available to the parties, widespread use of modern electronic discovery tools, such as technology-assisted review, should be encouraged, where appropriate. Such tools may include predictive coding, assisted review, centralized storage platforms, and analytics tools including, for example, email threading and concept clustering.

3. The Arbitral Participants should also consider leveraging technology solutions to secure their Documents and Evidence during collection, Processing, and disclosure,

to ensure the timely and secure destruction of Documents and Evidence once proceedings have closed, and generally to comply with Data Protection Laws and protect the privacy rights of relevant Data Subjects. For example, where possible, the parties should maintain Documents and Evidence only on secure servers, rely on third-party data processors with advanced data security infrastructures, and employ technology solutions that can assist in identifying and, where necessary, redacting or otherwise protecting Personal Data.

4. The parties should agree on appropriate formats for production that, where possible, include a text-searchable load file. Additionally, they should agree on a production protocol listing the metadata fields to be produced with Documents and Evidence and the kinds of Protected Data to be redacted.

Principle 3: An agreement between the parties as to the scope of document disclosure should be respected by an Arbitral Tribunal, provided their agreement is consistent with Principles 1 and 2.

Comment

Principle 3 recognizes that party consent and autonomy are hallmarks of International Arbitration, facilitating the benefits that make it an appealing mechanism of dispute resolution. Accordingly, and consistent with *The Sedona Conference Cooperation Proclamation*, Principle 3 encourages parties to come to an agreement as to the scope of disclosure that conforms with the tenets recognized in Principles 1 and 2. In particular, such disclosure should be limited to that which is lawful, necessary, and proportional to the needs of the dispute, so as to ensure cost-effectiveness and efficiency and foster the principles of data minimization.

Should the parties reach such an agreement falling within Principles 1 and 2, the Arbitral Tribunal should respect it—while working with the parties to improve it where it would be possible and appropriate to optimize arbitral efficiencies and avoid waste of resources—and ensure that it is followed throughout the arbitration process.

Principle 4: Where document disclosure is considered appropriate, and the parties are not able to agree on the scope of the disclosure, or if the agreement they propose is inconsistent with Principles 1 or 2, the Arbitral Tribunal should apply Principles 1 and 2 in deciding the extent of disclosure to be ordered.

Comment

This Principle recognizes that tension may exist between pure party autonomy and the goal of efficiency. To the extent that parties are unable to come to an agreement as to the scope of disclosure consistent with Principles 1 and 2, Principle 4 encourages Arbitral Tribunals to take steps to limit disclosure to that which is consistent with Principles 1 and 2, as appropriate considering the needs of the particular proceeding. For example, unless explicitly precluded from doing so by the parties' arbitration agreement, Arbitral Tribunals should consider requiring requesting parties to:

A. describe their requests with specificity and narrowly tailor requests so that they are directly tied, and material, to a particular claim or defense and its resolution;

B. restrict requests to specific custodians;

C. restrict requests to specific time periods;

D. limit the number of requests; and

E. minimize the Processing of Protected Data where possible.

Additionally, the Arbitral Participants should utilize methods to limit obtrusive requests for disclosure—for example, by imposing limits against requests that seek data that a) is in the hands of the party making the request, b) is not readily or reasonably available, or c) would impose an undue burden or expense, or implementing a protocol to shift or allocate to the requesting party the costs of an expensive undertaking to acquire such data.

Arbitral Participants should avoid overly broad requests for "any and all documents" on a subject. While parties might even agree on an expansive approach to disclosure, such a broad scope would be inconsistent with the goals of Principles 1, 2, and 4 and may be incompatible with applicable Data Protection Laws. Arbitral Tribunals should consider prohibiting such disclosure unless the requesting party can explain why the requested information is relevant to the claims or defenses, would be material to a resolution of a claim or defense, and proportional to the needs of the proceeding. They may also require requesting parties to affirm that their requests are not interposed for an improper purpose—such as extending the proceedings or increasing the costs—and allow responding parties the opportunity to object on the specific grounds that a request is overbroad, irrelevant, unduly burdensome or costly, subject to a valid privilege, or disallowed under applicable Data Protection Laws.

Another technique the Arbitral Tribunal may use to encourage reasonable and proportionate disclosure of relevant documents is to invite the parties themselves (in addition to their counsel) to attend case management conferences where the issues are discussed so that there is transparency about the potential costs and burdens of disclosure.

Arbitral Tribunals should also be wary of potential attempts by parties to weaponize the Data Protection Laws by using them

as a shield to prevent disclosure of damaging information or to otherwise disrupt the arbitral process. For example, when a party refuses to produce Documents and Evidence that have been ordered by the Arbitral Tribunal, arbitrators may use their discretion and power to draw adverse inferences and, where necessary as a last resort, impose sanctions.

Using these techniques strikes an appropriate balance among the principles of party autonomy, arbitral efficiency, and respecting the Data Protection Laws and the privacy interests of Data Subjects and Arbitral Participants. To achieve these objectives, at the outset of an International Arbitration, the Arbitral Participants should have an open dialogue about the data Processing and disclosure protocols to be followed during the arbitration. For example, a disclosure schedule and information security and data breach protocol should be established and should leverage data security advancements, data minimization principles, and document review technologies, when appropriate, to ensure that review and disclosure processes are responsibly and efficiently handled in compliance with applicable Data Protection Laws. The appropriate balance can be achieved by adopting a procedural order, terms of reference, or data protection protocol to ensure orderly proceedings.

Such schedules and protocols should consider, among other things:

A. which Data Protection Laws should be applied to the arbitration (recognizing that multiple Data Protection Laws may apply);

B. necessary categories of Personal Data to be processed and disclosed (if any) during the course of the arbitration, as well as the lawful bases for Processing and disclosing the information;

C. which Arbitral Participants will be considered the controllers of the data and how they will oversee any data processors (recognizing that multiple Arbitral Participants may be considered controllers);

D. whether cross-border transfers will be required during the review and disclosure process and, if so, how adequate protections will be guaranteed and under what legitimizing transfer mechanism, if applicable; and

E. the document review and retention protocols that will be implemented to ensure the efficient review and timely destruction of data.

To the extent that the parties cannot agree on data review and disclosure protocols—or are unable to resolve disputes related to data review and disclosure on their own—the Arbitral Tribunal should step in and, in the process, ensure that the rights of all parties are respected and the rights of Data Subjects under applicable Data Protection Laws are proportionally considered in the context of the particular case.

Principle 5: Applying Data Protection Laws to arbitration proceedings may require the Arbitral Tribunal to issue binding Data Protection Directions on the parties applicable to the Data Protection Laws at issue. The Arbitral Tribunal should consider issuing such directions after judging the parties' conduct under a standard of good faith, reasonableness, and proportionality, taking into account the considerations in Principles 1-4. While not binding on them, courts and Data Protection Authorities should respect and give reasonable deference to the decisions of the Arbitral Tribunal as to the application of Data Protection Laws to the Processing of Protected Data in International Arbitrations.

Comment

The nature of International Arbitration, as mentioned in Section III.H. above, is such that the Arbitral Tribunal must have the authority to issue binding directives on the parties with respect to the procedure and substance of the dispute. In a case where Data Protection Laws apply, this may require the Arbitral Tribunal to decide how data protection compliance will be addressed. These decisions should be enshrined in written Data Protection Directions in an agreed-upon form that are binding on the parties. Provided those decisions are made in good faith and are reasonable, courts and Data Protection Authorities should respect those decisions and give them reasonable deference.[11]

11. With that being said, Principle 5 in no way suggests that Arbitral Participants can or should proceed with data Processing activities inconsistent

Accordingly, Principle 5 encourages any Arbitral Participant that considers itself bound by a Data Protection Law to inform the other Arbitral Participants as soon as practicable during the proceedings to permit the arbitration to be undertaken in a manner that will maximize data protection compliance while minimizing impacts or burdens on the arbitration. To the extent that other Arbitral Participants do not believe a Data Protection Law applies, they should promptly object to the application. The Arbitration Tribunal should be considered as having the authority to rule on such issues of applicability, and the Arbitral Participants should respect such rulings.

Arbitral Participants may not be subject to the same Data Protection Laws, and some participants may not be subject to any Data Protection Law at all. Moreover, parties may seek to use data protection compliance obligations to their advantage. Principle 5 recognizes the importance of addressing and documenting the resolution of data protection issues that may arise during an International Arbitration in written Data Protection Directions applicable to the specific matter. Addressing these issues early in writing, where possible, will enable better compliance while reducing the burden on the orderly conduct of the arbitral proceedings.

Principle 5 also recognizes the importance of Arbitral Participants maintaining a record of their data protection compliance efforts in a manner that can be shared with Data Protection Authorities, demonstrating that data protection obligations have been addressed and that reasonable, good-faith efforts have been made to institute data protection safeguards during the

---

with Data Protection Laws. Where necessary pursuant to applicable Laws, Arbitral Participants should seek approvals from Data Protection Authorities regarding Processing activities and, in any event, they should always carefully consider their obligations under Data Protection Laws.

arbitration proceedings. Data Protection Directions should address the following topics, where appropriate:

A. The lawful basis for data Processing.

B. The lawful basis for data transfer.

C. The exchange of Documents and Evidence.

D. Any data security requirements and data breach protocols.

E. Management of Data Subject rights.

F. Notification obligations.

G. Documentation of data protection compliance.

H. Any use of online case management platforms to assist with data management and data protection compliance.

Principle 6: Arbitral Participants should put in place technical and organizational measures appropriate to ensure a reasonable level of information security of the Documents and Evidence, taking into account the scope and risk of the Processing, the capabilities and regulatory requirements of the Arbitral Participants, the costs of implementation, and the nature of the information being Processed or transferred, including whether it includes Protected Data, privileged information, or sensitive commercial, proprietary, or confidential information.

Comment

Principle 6 contextualizes information security as encompassing the measures that the Arbitral Participants should consider taking to minimize the risks of both unauthorized disclosures of data and cyberattacks. It, therefore, encourages the Arbitral Participants to adopt a protocol to manage information security and promote compliance with Data Protection Laws.

Among the measures that Principle 6 encourages the Arbitral Participants to consider including in such an information security and data breach protocol, in a manner consistent with the other Principles, are the following:

A. Procedural and operational controls to limit access to and proliferation of Protected Data, consistent with industry standards for information governance, data retention, and data destruction.

B. Technical controls including, but not limited to, strong password protocols, data security

awareness training, access controls, encryption of data in transit and at rest, redaction, anonymization, or pseudonymization of Protected Data.

C. Minimization or restriction of uses or transport of unencrypted removable media such as USB stick drives, CDs, DVDs, and external hard drives.

D. Centralization of communications, data storage, and collaboration tools to software applications and service providers with appropriate data security and procedural certifications.

E. Preventative and mitigating cyberattack controls including, but not limited to, encryption, perimeter integrity, operational monitoring, incident response, and insurance coverage.

V. CONCLUSION

The six Principles of International Arbitration presented in this publication address the secure processing, review, and disclosure of data—particularly Personal or other Protected Data—in the specific context of document disclosure in international commercial arbitration. The Principles are intended to provide a reasonable and proportional approach to the use and protection of data in international arbitration that: (1) respects the data protection and privacy rights of relevant Data Subjects while at the same time recognizing the due process rights of the Arbitral Participants, including the right of parties to adduce evidence material to resolution of the matter; and (2) ensures reasonable and good-faith compliance with Data Protection Laws, while simultaneously respecting the quasi-judicial role of International Arbitration and ensuring that arbitral proceedings are not unduly hindered. By adopting these six Principles of International Arbitration, participants can better mitigate potential conflicts with privacy laws and regulations in the context of cross-border data transfers during International Arbitration proceedings.

ARTIFICIAL INTELLIGENCE IN HEALTHCARE: A SURVEY OF FEDERAL AND STATE LAWS

By Eleanor T. Chung and Stuart M. Gerson

Eleanor T. Chung is a litigation associate at Epstein Becker & Green, P.C., specializing in artificial intelligence and fraud and abuse in the health care and life sciences industries. She co-leads the firm's Artificial Intelligence in Litigation group, and she is the co-author of *Pleading Causes of Action in Maryland* (7th ed.), a widely cited treatise on Maryland civil procedure.

Stuart M. Gerson is Of Counsel at Epstein Becker & Green, P.C., where he specializes in cybersecurity, artificial intelligence, and False Claims Act litigation. He previously served as the U.S. Assistant Attorney General for the Civil Division and as Acting U.S. Attorney General under President Clinton, following his appointment in the Bush administration.

This publication may be cited as follows:

Eleanor T. Chung and Stuart M. Gerson, *Artificial Intelligence in Health Care: A Survey of Federal and State Laws*, 26 SEDONA CONF. J. 481 (2025).

To date, there has been little definitive activity concerning the regulation of Artificial Intelligence ("AI") applications at the Federal level. Most Federal attention has focused on child pornography, intellectual property and fraud-related matters such as deep fakes and copyright infringement. To the extent that political nature abhors a regulatory vacuum, most of the action shifted to the States, as we describe. And, as was the case with cybersecurity and data privacy, where Federal legislative activity initially was muted, the States were heavily influenced by European Union law, particularly the General Data Protection Regulation ("GDPR"), as the archetype for their own expansive legislative and regulatory activities.

The GDPR establishes guidelines for how organizations handle personal information, including requirements for consent, data security, and the right to access and delete data. Many of the U.S. State laws that are modeled on the GDPR allow private rights of action to enforce them. Despite industry groups' heavily lobbying for Federal preemption and the establishment of corporate safe harbors based upon demonstrable regulatory compliance, there has been no such national privacy or data security law enacted by the Congress.

Until recently, the situation has been much the same in the United States on the AI front. Though there are various regulatory guidelines published by agencies like the National Institute of Standards and Technology ("NIST"), Cybersecurity and Infrastructure Security Agency ("CISA"), and the Departments of Commerce and the Treasury, there is no comprehensive, preemptive Federal law governing the use and abuse of AI. There is some regulation by litigation, *e.g.*, with the use of employment discrimination laws to combat alleged AI algorithmic bias. However, in the larger sense, the pattern that obtained with respect to privacy and security has repeated itself with AI, in this case with the EU AI Act serving as the model for the many States that have promulgated AI laws of their own. The

European model is based upon the classification of AI programs according to their risk, and most of the obligations fall upon developers. Again, one finds criticism among providers that there is no federal preemption, or safe harbors.

On July 4, 2025, President Trump signed into law the so-called "One Big Beautiful Bill Act," from which the Senate had removed a House-passed provision that would have established a ten-year moratorium on the States' enforcing any law or regulation affecting "artificial intelligence models," "artificial intelligence systems," or "automated decision systems."[1] Although Congress retains the theoretical ability to preempt state AI law in order to obtain nationwide regulatory and enforcement uniformity, it has chosen not to do so. Accordingly, all fifty states, as well as the District of Columbia, Puerto Rico and the Virgin Islands, have passed, or have introduced, legislation intended to regulate AI.[2] By removing the moratorium from the bill, Congress has left the way open for the States and territories to continue to enact and enforce AI-related statutes as well as perpetuating both state and private actions asserting *e.g.*, discrimination, negligence and other tort law, under state statutory and common law authority. But that is not the end of things with respect to AI.

Although there is little apparent energy within Congress to take a leadership position respecting global regulation and promotion of AI, the adage that "nature abhors a vacuum" has

1. *Compare* H.R. 1, 119TH CONG. § 43201(c) (as passed by House, May 22, 2025) (imposing 10-year state AI enforcement moratorium), *with* H.R. 1, 119th Cong., Pub. L. No. 119-21, 139 Stat. 72 (2025) (reflecting absence of the moratorium).

2. *See, e.g.*, National Conference of State Legislatures, *Report: Legislation Related to Artificial Intelligence*, available at https://www.ncsl.org/technology-and-communication/legislation-related-to-artificial-intelligence (site visited Aug. 18, 2025).

come to apply to recent activity, not just among the states and territories, but within the executive branch of the national government. Thus, on July 23, 2025, the Trump White House issued an Artificial Intelligence (AI) Action Plan that the administration asserts will assure American "global AI dominance." The president accompanied this Plan with three AI-delated Executive Orders aimed at: 1) "Accelerating Federal Permitting of Data Center Infrastructure"; 2) "Promoting the Export of the American Export AI Technology Stack"; and 3) "Preventing Woke AI in the Federal Government."

The AI Action Plan sets forth three nominal pillars intended to accelerate AI innovation, build American AI infrastructure, and assure American leadership in AI diplomacy and security.[3] Notwithstanding that the moratorium on state activity did not survive in Congress, the AI Action Plan attempts to limit federal funding of AI activities in states with burdensome regulatory regimes.[4] Health care providers should be particularly concerned that the administration is attempting to block recipients of federal funds from employing AI policies and Large Language Models that promote misinformation; Diversity, Equity and Inclusion; and climate change.[5] This strong policy directive implies that entities using AI in diagnosis and treatment decision-making and provision of health care services are at risk of both governmental and private *qui tam* relator actions under the federal False Claims Act, alleging false certification of compliance with applicable laws and regulations where providers use of AI promotes claimed reverse discrimination or otherwise

3. *America's AI Action Plan* (July 23, 2025), THE WHITE HOUSE, https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

4. *Id.*

5. *Id.*

offends administration views of what constitutes ideological neutrality.

On the other hand, certain large health care providers and insurers may see benefits resulting from the AI Action Plan's intended stimulation of AI research facilities, data centers and alternative energy sources.

We have limited our survey of state AI laws to those that affect the practice of health care and the life science industries. State AI laws that do not directly govern providers or payors, or the practice of medicine or reimbursement, are omitted from this survey. *E.g.*, those laws that create a task force to study the effects of artificial intelligence, or establish an Office of Artificial Intelligence, which may, at a later date, promulgate a regulation or guidance affecting the health care and life sciences industries, are not described herein. Our survey presents each law followed by a concise summary of its associated risks and means of enforcement.

Also note that, generally, all state AI health care laws must be read in tandem with a mosaic of state privacy, anti-discrimination, and consumer protection statutes.

I. CALIFORNIA

A. California's Artificial Intelligence in Health Care Services

1. The law

California Governor Gavin Newsome signed into law Assembly Bill 3030 ("AB 3030"), also known as the Artificial Intelligence in Health Care Services ("AIHCS") law, on September 28, 2024. This law was intended to prevent scenarios where a patient believes he or she is communicating with a provider but is in fact communicating with generative AI. Effective January 1, 2025, AIHCS imposes a two-fold disclosure requirement for health care facilities, clinics, physician's offices, and group

practices using generative AI to communicate regarding clinical information.[6]

First, providers using generative AI to "generate written or verbal patient communications" regarding clinical information must include a disclaimer in written and audiovisual communications disclosing the use of the AI.[7] If the communication is written, the disclaimer must appear "prominently at the beginning of each communication."[8] If the communication is a "continuous online interaction[,]" such as a with a chatbot, the disclaimer must be "prominently displayed throughout the interaction."[9] If the communication is aural, the disclaimer must be provided verbally, at the start and end of the communication.[10] If the communication is via video, the disclaimer must be "prominently displayed throughout the interaction."[11]

Second, providers using generative AI must provide "clear instructions describing how a patient may contact a human health care provider" employee.[12]

The law does *not* apply if the communication itself is created by Generative AI "and read and reviewed by a human licensed or certified health care provider[.]"[13] Professional associations backed this provision, fearing that without it, providers may be deterred from leveraging AI's time-saving benefits for routine tasks made more efficient through automation.[14] Note that the

6. CAL. HEALTH & SAFETY CODE § 1339.75.
7. *Id.* at § 1339.75(a).
8. *Id.* at § 1339.75(a)(1)(A).
9. *Id.* at § 1339.75(a)(1)(B).
10. *Id.* at § 1339.75(a)(1)(C).
11. *Id.*
12. *Id.* at § 1339.75(a)(2).
13. *Id.* at § 1339.75(b).
14. California Bill Analysis, A.B. 3030 Assem., 6/26/2024.

law does not apply to purely administrative communications for this reason.

2. Risk and enforcement

The Medical Board of the State of California and the Osteopathic Medical Board of California have jurisdiction over AIHCS. Thus, the penalties for violation of AIHCS are the panoply of disciplinary options available to the California Medical Board and Osteopathic Medical Board, which include license revocation, suspension of the right to practice, placement on probation, public remand, and any other action an administrative law judge may deem proper.[15]

While the authors have not identified a provider censored under AIHCS to date, providers censored for failure to maintain adequate and accurate medical records abound. It would be reasonable to expect that a provider that violates AIHCS also would violate the provision of the Business and Professions Article requiring physicians and surgeons to "maintain adequate and accurate records relating to the provision of services to their patients for at least seven years" from the date of service, and that penalties for violation of AIHCS would be on par with penalties for violation of this provision.[16] Generally speaking, penalties meted by the Medical Board correspond to the severity of harm to the patient and whether the offense was isolated or one of many.

15. CAL. BUS. & PROF. CODE § 2227; Cal. Code Regs. tit. 16, § 1663.

16. CAL. BUS. & PROF. CODE § 2266.

B. Physicians Make Decisions Act

1. The law

California Governor Gavin Newsome signed into law Senate Bill 1120 ("SB 1120"), also known as the Physicians Make Decisions Act ("PMDA") on September 30, 2024. Effective January 1, 2025, the bill requires human oversight of utilization decisions made by AI tools. PMDA is one of many state laws tackling prior authorization and utilization review, and is one of the few, including laws described herein from Illinois, Maryland, Nebraska, and Texas, to have passed.[17]

---

17. Much proposed state legislation tackling prior authorization has died on the vine. *See* Georgia HB 887 (failing *sine die* in the 2023-24 Regular Legislative Session, and seeking to prohibit AI from, *inter alia*, deciding insurance coverage*); see also* Illinois HB 5918 (failing *sine die* in the 2023-24 Regular Legislative Session, captioned "AI Use in Health Insurance Act," and establishing regulatory oversight of insurers including the insurers' use of AI systems to support adverse determinations); Indiana HB 1620 (failing *sine die* in the 2023-24 Regular Legislative Session, captioned "Disclosure of artificial intelligence use in health care," and requiring, *inter alia*, insurers to disclose the use of artificial intelligence); *see also* New Jersey S 1402 (failing *sine die* in the 2023-24 Regular Legislative Session, captioned "Prohibits certain discrimination by automated decision systems," and seeking to preclude discrimination by financial lenders, insurers, and providers from using automated decisions systems to discriminate against protected classes); *see also* New York A 9149 (failing *sine die* in the 2023-24 Regular Legislative Session, captioned "Relates to the use of artificial intelligence for utilization review," and establishing notice requirements for insurers and Health Maintenance Organizations using AI for utilization review); *see also* OK HB 3577 (failing *sine die* in the 2023-24 Regular Legislative Session, captioned "Artificial Intelligence Utilization Review Act," and requiring disclosure of AI used in utilization review to the Oklahoma Insurance Commissioner to certify that the algorithms and training data sets have minimized the risk of bias based on race, religion, ancestry, age, sex, etc.); *see also* Pennsylvania HB 1663 (failing *sine die* in the 2023-24 Regular Legislative Session, captioned "Regulation of Artificial Intelligence (AI) Use in Health Insurance Claims Processes" and requiring disclosure of the use of AI, requiring a human to provide the reason for a denial of a claim,

The law modifies the Knox-Keene Health Care Service Plan Act of 1975 ("Knox-Keene"), which imposes certain requirements on health plans: under Knox-Keene, plans must obtain a license from California's Department of Managed Health Care, maintain financial solvency, maintain provider networks sufficient to ensure timely care, and provide standardized benefits. Importantly, the Knox-Keene Act provides consumer protections, such as the right to independent medical review if a plan denies coverage for a medical treatment. By way of context, the Knox-Keene Act was one of the first state law answers to the federal Health Maintenance Organization Act of 1973, signed into law by President Richard Nixon.

The PMDA contains disclosure, anti-discrimination, and consumer protection provisions, and is a medley of humdrum reiteration of existing law (*e.g.*, mandatory disclosure of utilization review processes, tools must "not discriminate: in violation of state and federal law) and lofty, yet vague, ambitions (*e.g.*, the tool must not "cause harm" to an enrollee).

Specifically, the PMDA requires compliance with existing disclosure provisions, which mandate disclosure of "the policies, procedures, and a description of the process" used for approving, modifying, delaying, or denying medical necessity.[18] It also mandates that the artificial intelligence, algorithm, or other tool used of utilization review render judgement based on an enrollee's clinical history, the clinical circumstances as presented by the requesting provider, and the medical record, rather than relying solely on a group dataset.[19]

---

and requiring insurers to submit AI algorithms and training datasets to the Pennsylvania Department of Insurance for certification that the data sets have minimized the risk of bias pursuant to Pennsylvania anti-discrimination statutes).

18. CAL. HEALTH & SAFETY CODE §§ 1365.5, 1367.01(b), (k).

19. CAL. HEALTH & SAFETY CODE § 1367.01(k).

Human review of decisions by artificial intelligence is also mandated; the tool is not permitted to make decisions of medical necessity.[20] The tool must not discriminate in violation of state or federal law, must be applied equitably, and must be open to inspection for audit or compliance reviews. Lastly, the tool must not "directly or indirectly cause harm" to an enrollee.[21]

2. Risk and enforcement

Enforcement mechanisms of the PMDA include an array of administrative, civil, and criminal penalties.

A plan that no longer meets the standards set out in Section 1367 *et seq.* is subject to disciplinary action, including administrative and civil penalties, one of the most severe of which is suspension or revocation of any license.[22] An individual who violates provisions governing health services plans is liable for a civil penalty of up to $25,000 per violation.[23] As the nature of artificial intelligence and algorithmic utilization review tends to engender consistent or clustered errors, rather than one-offs, a violations of the PMDA could be very expensive.

A willful violation of the Knox-Keene Act is a crime. Penalties include a fine of up to $20,000, imprisonment in state or county jail for not more than one year, or both.[24]

---

20. *Id*. at § 1367.01(k)(1)(D) (stating that a plan must ensure that "the artificial intelligence, algorithm, or other software tool does not supplant health care provider decision-making"); *id*. at 1367.01(k)(2) (stating that the tool "shall not deny, delay, or modify health care services based, in whole or in part, on medical necessity").

21. *Id.* at § 1367.01(k)(1)(K).

22. CAL. HEALTH & SAFETY CODE § 1386(a).

23. *Id.* at § 1387(a)(1).

24. CAL. HEALTH & SAFETY CODE § 1390.

Guidance on how to comply with the PMDA may be forthcoming. The Act provides that the California State Department of Health Care Services, within one year of the Act's passing, may provide guidance on implementation of the new law.[25] This guidance will be sub-regulatory and not subject to the Administrative Procedure Act.[26] As of this writing, no guidance has been issued.

II. COLORADO

A. Colorado's AI Act

1. The law

Colloquially known as "Colorado's AI Act," Senate Bill 24-205, "An Act Concerning Customer Protections for Interactions with Artificial Intelligence" was signed into law by Colorado Governor Jared Polis on May 17, 2024. Effective February 1, 2026, Colorado's AI Act is the second major state artificial intelligence law, after Utah's Artificial Intelligence Policy Act, enacted about two months prior, on March 13, 2024.[27] It is widely considered to be one of the most, if not the most, comprehensive state AI laws. Other states that have attempted but failed to pass omnibus AI Acts include New Mexico and Virginia.[28]

---

25. *Id*. at § 1367.01(k)(1)(K)(5).

26. *Id*.

27. *See infra* Utah.

28. *See* Virginia HB 2094 (failing on April 2, 2025 due to Governor Glen Youngkin's veto, which described the bill which would have, *inter alia*, adopted the National Institute of Standards and Technology ("NIST") framework for operation of AI systems, as "burdensome" and risking "turning back the clock on Virginia's economic growth, stifling the AI industry as it is taking off"); *see also* New Mexico HB 60 (failing *sine die* in the 2025 Regular Legislative Session and, like Colorado's AI Act, defined "high-risk AI systems" and imposed transparency and disclosure requirements).

Perhaps the most emblematic of Justice Brandeis's "laboratories of democracy" metaphor, the Colorado AI Act is a concoction of state and European AI laws. It borrows some attributes of the European Union's ("EU") AI Act, which was adopted by the European Parliament on March 13, 2024, and became effective on August 1, 2024. It also incorporates California Privacy Protection Act draft regulations and New York's Local Law 144 of 2021 which governed Automated Employment Decision Tools.[29]

Whereas the EU AI Act divides AI systems into "unacceptable risk" (*e.g.*, social scoring, predictive policing, facial recognition via data scraping, etc.), "high-risk" (*e.g.*, essential private services and public services), and "limited risk" (*e.g.*, chatbots), Colorado's AI Act contemplates only "high-risk" uses and other uses. A high-risk AI system under Colorado's AI Act is "any artificial intelligence system that, when deployed, makes, or is a substantial factor in making, a consequential decision."[30] A "consequential decision" is defined as a decision that has a "material legal or similarly significant effect" on the provision or denial of:

- Educational enrollment or opportunity
- Employment or employment opportunity
- A financial or lending service
- An essential government service
- Healthcare services
- Housing
- Insurance, or

29. *See* Draft Automated Decisionmaking Technology Regulations (Dec. 2023), available at https://cppa.ca.gov/meetings/materials/20231208_item2_draft.pdf; *see also* Local Law No. 144 of 2021, 2020 N.Y. City Council Int. No. 1894-A (codified at N.Y. City Admin. Code § 20-870, *et seq.*).

30. COLO. REV. STAT. ANN. § 6-1-1701(9)(a).

- A legal service.[31]

Also like the EU AI Act, the Colorado Act furnishes different obligations for developers versus deployers.

Notably, there is some prophylactic protection for deployers: there is a rebuttable presumption that a deployer used reasonable care if it complied with the mandates of the Act.[32] To so abide, the Act mandates a compliance program: a deployer must "implement a risk management policy and program to govern the deployer's deployment of the high-risk artificial intelligence system" which can mitigate and reasonably foresee the risks of algorithmic discrimination.[33] Impact assessments are required annually and whenever there is a "substantial modification" to the artificial intelligence system.[34]

2. Risk and enforcement

The grand scope of Colorado's AI Act is perhaps disproportionate to its teeth. The Act provides no private right of action. Enforcement remains the exclusive authority of the Colorado attorney general,[35] although actions may also be brought by state district attorneys.[36] A violation of the Act constitutes an unfair trade practice under existing Colorado law and is punishable by a fine of up to $20,000.[37]

With an effective date in the coming year, we must wait and see how enforcement will unfold. Colorado's attorney general is widely perceived as one of the more active state attorneys

31. *Id.* at § 6-1-1701(b)(II)(3).
32. *Id.* at § 6-1-1703(1).
33. *Id.* at § 6-1-1703(2).
34. *Id.* at § 6-1-1703(3)(a)(II).
35. COLO. REV. STAT. ANN. § 6-1-1706
36. *Id.* at § 6-1-103.
37. *See id.* at §§ 6-1-105, 6-1-112.

general. A cursory review of Consumer Protection Acts resolved by the Colorado Attorney General reveal about a half dozen data protection settlements and a few unlawful loan servicing settlements in the last four years.[38]

III. GEORGIA

A. Artificial Intelligence & Biometric Technologies

1. The law

On July 7, 2023, Georgia Governor Brian P. Kemp signed into law House Bill 203 ("HB 203"), one of the health care and life sciences laws surveyed here with the narrowest application. HB 203 amends Section 31-12-12 of the Health Article captioned "Ocular health; eye assessments; prescription of contact lenses or spectacles."[39]

Prior to 2023, Georgia law required contact lenses to be sold in a face-to-face transaction.[40] Today, contact lenses must be fitted during an in-person eye examination, but the dispensing of replacement contacts need not occur at a face-to-face appointment. HB 203 permits an ophthalmologist to use an "assessment mechanism" to conduct an eye assessment or to generate a prescription for contact lenses or glasses. An "assessment mechanism" is defined as an in-person or telemedicine appointment wherein the ophthalmologist uses "automated or virtual equipment, application, or technology designed to be used on a telephone, a computer, or an internet accessible device[,]" which

38. *See* Consumer Protection Cases, available at https://coag.gov/office-sections/consumer-protection/consumer-protection-cases.

39. GA. CODE ANN. § 31-12-12.

40. *See* James C. Cooper, Public Versus Private Restraints on the Online Distribution of Contact Lenses: A Distinction with A Difference, 3 J.L. ECON. & POL'Y 331, 338 (2007); *see* also HB 775 (2016).

includes "artificial intelligence devices and any equipment, electronic or nonelectronic, that are used to conduct an eye assessment."

2. Risk and enforcement

HB 203 is notable because optometrists' scope of practice is broadened to include eye examinations utilizing artificial intelligence. This is one of the first state AI laws that could be said to bear on practitioner standard of care; an enterprising attorney could surely argue in malpractice or other contexts that artificial intelligence is an accepted part of an eye examination.

IV. ILLINOIS

A. Ins-Adverse Determination

1. The law

On July 19, 2024, Illinois Governor J.B. Pritzker signed into law House Bill 2472 ("HB 2472"), captioned Ins-Adverse Determination, one of the few state laws tackling prior authorization and utilization review to have passed.

Effective January 1, 2025, HB 2472 was passed to ensure transparency in prior authorization programs and to prevent such programs from hindering health care providers' independent medical judgment.[41] HB 2472 augments, *inter alia*, the Illinois Prior Authorization Reform Act, signed into law by Governor J.B. Pritzker on August 19, 2021, and effective January 1, 2022. The initial act mandated that fully insured non-HMO plans and Illinois Medicaid plans respond to prior authorization requests within specific timeframes (five days for non-urgent services, and within 48 hours for urgent services); assigned validity periods (approved prior authorizations are valid for six months, and

41. 215 Ill. Comp. Stat. Ann. 200/5.

for chronic conditions, twelve months); and created transparency requirements regarding which services require prior authorization; codified the appeals process.[42]

Under HB 2472, adverse medical necessity determinations made by AI must be reviewed by a human, clinical peer.[43] The new law also broadens definitions of "adverse determination" and "final adverse determination" to include decisions made with algorithmic processes. 215 Ill. Comp. Stat. Ann. 180/10. To prevent wasteful and duplicative barriers to care, HB 2472 prohibits insurers from requiring both the plan enrollee and his or her healthcare provider from having to obtain prior authorization for the same instance of a health care service. 215 Ill. Comp. Stat. Ann. 200/55(e).

2. Risk and enforcement

There is no private right of action. 215 Ill. Comp. Stat. Ann. 200/85. The Illinois Department of Insurance is tasked with administration and enforcement, and may impose a fine not to exceed $250,000 for failure to submit a plan of correction, failure to abide by a plan of correction, or for repeated violations of the Prior Authorization Reform Act. *Id.* Individuals who believe that his or her insurer is in violation of the Act may file a complaint with the Department of Insurance which will trigger an investigation.[44]

42. *See generally* Illinois Prior Authorization Reform Act (200/1 to 200/999).

43. 215 Ill. Comp. Stat. Ann. 134/85(e).

44. *Id.*

A. House Bill 1806 – Therapy Resources Oversight/ Wellness and Oversight for Psychological Resources Act

1. The law

On August 1, 2025, Governor J.B. Pritzker signed into law House Bill 1806 ("HB 1806"), the Therapy Resources Oversight Act ("TROA"), which became effective the same day. TROA outlines the permitted uses of AI in therapy services: AI may be used for "administrative support" or "supplementary support" in therapy or psychotherapy services, as long as the licensed professional "maintains full responsibility for all interactions, outputs, and data associated with the system."[45]

Further, a provider may not use AI for supplementary support at all if the session is recorded or transcribed, unless the patient is provided notice and the patient consents to the use of the AI.[46] TROA specifically proscribes the use of AI for therapeutic decision-making, client interaction "in any form of therapeutic communication[,]" for generating client treatment plans without review and approval by a licensed professional, and for the purpose of detecting emotions or mental states.[47]

"Administrative support" is defined by the Act to include tasks that assist a licensed professional in the provision of therapy and psychotherapy services, but not "involve communication[.]"[48] Examples of such tasks include, but are not limited to, appointment scheduling, processing billing and insurance claims, and "drafting general communications related to therapy logistics that do not include therapeutic advice."[49]

---

45. 225 Ill. Comp. Stat. Ann. 155/15(a).
46. *Id*. at 155/15(b).
47. *Id.* at 155/20.
48. 225 Ill. Comp. Stat. Ann. 155/10.
49. *Id.*

"Supplementary support" is defined by the act to include tasks that are not administrative, but are also not therapeutic services, which include, but are not limited to, maintaining client records, analyzing anonymized data to identify trends or track client progress, and identifying external resources for referrals.[50]

2. Risk and enforcement

There is no private right of action. Any individual or entity found to have violated the Act will pay a civil penalty of up to $10,000 per violation.[51] Penalties will be determined based on the degree of harm caused by the violation, as well as the circumstances.[52] The Department of Financial and Professional Regulation ("DFPR") has the "authority to investigate actual, alleged, or suspected violations of the Act."[53]

The DFPR publishes monthly disciplinary reports that enumerate violators of every type of regulated professional: health care providers, consumer lenders, insurers, barbers, athletes, accountants, engineers, *et al.* The reports provide the name of the licensed professional and a one-sentence description of the violation only. To date, the authors have not identified an AI-related violation.

50. *Id.*

51. *Id.* at 155/30(a).

52. *Id.*

53. *Id.* at 155/30(b).

V. MARYLAND

A. *House Bill 820 – Health Insurance – Utilization Review – Use of Artificial Intelligence*

1. The law

On May 20, 2025, Maryland Governor Wes Moore signed into law House Bill 820 ("HB 820"), which joins California's Physicians Make Decisions Act and Illinois's Ins-Adverse Determination Act as one of the first state laws to govern the use of AI in utilization review. Effective October 1, 2025, HB 820 amends Section 15-10A-06 of the Insurance Article, and requires payors, pharmacy benefit managers, and other entities that conduct utilization review to ensure that their AI tools base determinations on an individual's clinical background. Like California's law,[54] HB 820 aims to prevent adverse decisions based solely upon a group dataset.[55] Under HB 820, payors must include in their quarterly reports to the Maryland Insurance Commissioner whether AI, algorithms, or any other software tools were used in making an adverse decision. Also, like California's law, HB 820 states that the AI or tool should not replace the role of a provider for utilization review decision-making.

B. *Risk and Enforcement*

There is no private right of action. A person found to have willfully violated Maryland's Insurance Article is guilty of a misdemeanor and is subject to a fine not to exceed $100,000.[56] The Maryland Insurance Administration maintains an active

54. *Compare with* CAL. HEALTH & SAFETY CODE § 1367.01(k).

55. Bill sponsor Delegate Dr. Terri Hill explained that HB 820 aims to prevent care denials based on comparisons to group data sets. Panel Discussion. "Legislative Update." *James MacGill Inn of Court*, May 7, 2025.

56. MD. CODE ANN., INS. § 1-301.

docket, and has recently enforced the Insurance Article for violations ranging from redlining and discrimination, to misappropriation of insurer funds, to withholding of premiums. The agency does not post a comprehensive list of actions and orders.[57] The mechanisms and regularity of enforcement under HB 830 will undoubtedly be clarified over time as the law is implemented.

VI. NEBRASKA

A. Ensuring Transparency in Prior Authorization Act (Legislative Bill 77)

1. The law

On June 6, 2025, Nebraska governor Jim Pillen signed into law the Ensuring Transparency in Prior Authorization Act, effective January 1, 2026. As its name suggests, the Act emphasizes disclosure: a utilization review agent must disclose to the Department of Insurance, on its website, to each health care provider in its network, and to each enrollee whether AI is used or will be used in the utilization review process.[58] Note that other states (Oklahoma, New Jersey) have acts by the same name, but unlike Nebraska's Act, these acts do not discuss AI.

Nebraska's Act further mandates that AI must not be the sole basis by which care is denied, delayed, or modified based on medical necessity.[59] The Department is free to audit an insurer's automated utilization review management system at any time.[60]

---

57. *See* Md. Ins. Admin., Order and Exams Search, https://insurance.maryland.gov/Pages/decisions-orders.aspx ("The MIA posts many of those actions here.").

58. 2025 NEB. LAWS L.B. 77, § 12(2).

59. *Id.* at § 12(1).

60. *Id*. at § 12(3).

The Act amends prior authorization in many other ways not involving AI, which may in fact bear on how AI is used in utilization review. For example, the Act mandates that a utilization review agent's compensation may not be linked to volume of denials.[61] This language ensures that systematized denials, such as those that may be facilitated by AI, are not rewarded.

2. Risk and Enforcement

As the law becomes effective on January 1, 2026, enforcement at this time is speculative. The law does not enumerate a private right of action or penalties for violators.

VII. NEVADA

A. Assembly Bill 406

1. The law

On June 5, 2025, Nevada Governor Joe Lombardo signed AB 406, which, among other things, precludes AI from practicing mental and behavioral health services. Effective July 1, 2025, the law amends Title 39, the Mental Health Article, to prohibit any representation that artificial intelligence is "capable of providing professional mental" health care.[62] It also prohibits providers from representing that a user "may interact with any feature of the artificial intelligence system which simulates human conversation in order to obtain professional mental or behavioral health care" and from representing that AI itself is "a therapist, a clinical therapist, a counselor, a psychiatrist, a doctor[,]" or any other type of mental or behavioral health care provider.[63] The law prohibits AI programmed to provide mental

61. *Id*. at § 13.

62. Assemb. B. 406, 83d Leg., Reg. Sess. (Nev. 2025).

63. *Id.*

and behavioral health care services as "if provided by a natural person[.]"[64] Similar to the prohibition contained in the Healing Arts Chapter of the Professions, Occupations and Businesses Article, AB 406 includes a prohibition on the practice of mental and behavioral health care without credentialing.[65]

AB 406 specifically permits AI to be used for "administrative support," which include scheduling appointments, managing records, billing activities, analyzing data, and "organizing, tracking and managing files or notes relating to an individual session with a patient."[66] Any reports, data, or summaries generated by AI must be independently reviewed by the provider.[67]

2. Enforcement

There is no enumerated private right of action. AB 406 authorizes the Division of Public and Behavioral Health within the Nevada Department of Health and Human Services to investigate potential violations and to bring civil penalties of a maximum of $15,000 per violation.[68] In the month since the law took effect, the authors have identified neither fines nor disciplinary actions brought under it.

VIII. OREGON

A. HB 2748 – Relating to the Use of Nursing Titles

1. The law

On June 24, 2025, Governor Tina Kotek signed into law HB 2748, which becomes effective January 1, 2026. HB 2748 amends

64. *Id.*

65. *Id.*; *see* also NEV. REV. STAT. ANN. § 629.580.

66. Assemb. B. 406, 83d Leg., Reg. Sess. (Nev. 2025), at §§ 7(1)(6), 8.

67. *Id.* at § 8(4).

68. *Id*. at § 7 (4)-(5).

Section 678.010 to 678.410 of the Occupations and Professions Article, governing Professional Nurses. The very brief law states that "A nonhuman entity, including but not limited to an agent powered by artificial intelligence, may not use any of the following titles[,]" including advanced practice registered nurse, certified registered nurse anesthetist, clinical nurse specialist, licensed practical nurse, registered nurse, nurse practitioner, certified medication aide, or certified nursing assistant. The bill was introduced by Representative Travis Nelson, a registered nurse, after lobbying by the American Nurses Association.[69] Representative Nelson's testimony in support of HB 2748 emphasized that "an AI program is not licensed to deliver medical care," and thus "there would be no accountable party for any potential errors or mistakes in treatment."[70]

This law seeks to prevent AI from impersonating nursing clinicians, but unlike laws with similar aims in other states, it does not impose a disclosure requirement. Instead, HB 2748 seeks to preclude impersonation through licensure restrictions.

2. Risk and Enforcement

HB 2748 creates no private right of action. Any person found to have violated Section 678.010 to 678.410 is guilty of a Class C misdemeanor. The maximum time of imprisonment for a Class C misdemeanor is 30 days.[71] The maximum fine is $1,250.[72] The fine applies to individuals only, not to corporations.[73] The court may, instead of the fine, order the violator to pay an amount not

69. Hearing on H.B. 2748 before the H. Comm. On Behavioral Health and Health Care, 83rd Cong. (Or. 2025) (testimony of Rep. Travis Nelson).

70. *Id.*

71. O.R.S. § 161.615.

72. O.R.S. § 161.635.

73. *Id.*

to exceed double the amount the violator gained from committing the offense—although how this penalty would be enforced in the context of an AI impersonation case remains uncertain.

IX. RHODE ISLAND

A. The Consumer Protection In Eye Care Act

1. The law

On June 29, 2022, Rhode Island Governor Dan McKee signed into law the Consumer Protection in Eye Care Act ("CPECA"), which became effective immediately upon enactment.[74] Like Georgia's Artificial Intelligence & Biometric Technologies law, CPECA governs eye care in the state. It applies to all "assessment mechanisms," including AI "devices and any equipment, electronic or nonelectronic, that is used to perform an eye assessment."[75] To use such an assessment mechanism, a provider must, among other things, ensure that a patient has received an in-person eye exam within 24 months, conform to the standard of care.[76]

2. Risk and enforcement

The act provides no private right of action. A person found to have violated the act must pay a civil penalty not to exceed $10,000 per violation. Also, like Georgia's law, CPECA is one of the first state AI law that could be said to bear on practitioner standard of care; citing to CPECA, an enterprising attorney could surely argue in malpractice or other contexts that artificial intelligence is an accepted part of an eye examination.

---

74. *See* 23 R.I. GEN. LAWS ANN. § 23-97-1, *et seq.*

75. *Id.* at § 23-97-2(a)(1).

76. *Id.* at 23-97-4.

X. TEXAS

A. SB 815 – Relating to the Use of Certain Automated Systems in, and Certain Adverse Determinations Made in Connection with, the Health Benefit Claims Process

1. The law

On June 20, 2025, Texas Governor Greg Abbott signed into law Senate Bill 815, amending Section 4201.002 of the Texas Insurance Code by regulating automated decision-making in utilization review.[77] Effective September 1, 2025, the law entirely prohibits AI from making adverse determinations "wholly or partly."[78] Like other state laws enumerated here that prohibit AI from use in clinical or utilization decision-making, S.B. 815 permits AI to be used for administrative support, as well as for fraud detection.[79]

2. Risk and enforcement

There is no private right of action. The law imposes no additional penalties. The remedies and penalties under the Insurance Article include sanctions, cease and desist orders, and administrative penalties.[80] Sanctions include revocation of authorization to operate in Texas,[81] suspension of authorization to operate for up to one year,[82] administrative penalties, and any

77. Act of June 20, 2025, ch. ___, Tex. Gen. Laws ___ (codified at TEX. INS. CODE § 4201.156).

78. *Id.* at § 4201.156.

79. *Id*. at § 4201.156(c).

80. TEX. INS. CODE ANN. § 4201.603.

81. *Id.* at § 82.051.

82. *Id.* at § 82.052.

combination thereof.[83] Administrative penalties of up to $25,000 per violation may be imposed against violators.[84]

B. SB 1188 – Relating to Electronic Health Record Requirements; Authorizing a Civil Penalty

1. The law

On June 20, 2025, Texas Governor Greg Abbott also signed into law Senate Bill 1188, adding Chapter 183, Electronic Health Records, to the Health and Safety Article. [85] Also, effective September 1, 2025, the law establishes standards for Electronic Health Records ("EHRs") in Texas. The law mandates that EHRs are physically maintained in the United States or a United States territory; that records are accessible only to individuals performing duties within the scope of their employment; and that each entity must implement "reasonable and appropriate administrative, physical, and technical safeguards" to protect record confidentiality and integrity.[86] Section 183.005, captioned "Artificial Intelligence in Electronic Health Record," states that practitioners may use AI for diagnostic purposes and to recommend a course of treatment.[87] AI may be so used, however, only if the practitioner is acting within the scope of his or her license; the use of AI is not otherwise prohibited by state or federal law; and the practitioner reviews records created by the AI.[88]

Section 183.005 also imposes a disclosure requirement. The law mandates that a practitioner using AI for diagnostic

---

83. *Id.*

84. *Id*. at § 84.022.

85. Act of June 20, 2025, ch. ___, 2025 Tex. Gen. Laws ___ (codified at TEX. HEALTH & SAFETY CODE § 183.001 et seq.).

86. *Id.* at § 183.001.

87. *Id.* at § 183.005.

88. *Id.* at § 183.005(a).

purposes must disclose the use of that technology to his or her patients.[89] Notably, the law does is silent as to the form of disclosure—for example, whether it must be provided at the start of each patient encounter, placed on official letterhead, or prominently displayed at the facility.

2. Risk and enforcement

There is no private right of action. The law authorizes the attorney general to institute an action for civil penalties.[90] The appropriate regulatory agency may take disciplinary actions against an entity that violates the law three or more times.[91] Such disciplinary actions may include suspension or revocation of an entity's license, registration, or certification.[92]

The law also authorizes injunctive relief and civil penalties.[93] Civil penalties of $5,000 may be lodged for each negligent violation; penalties of $25,000 for each knowing or intentional violation; and $250,000 for each violation in which an entity knowingly or intentionally used protected health information for financial gain.[94]

XI. UTAH

A. Artificial Intelligence Policy Act

1. The law

On March 13, 2024, Utah Governor Spencer Cox signed into law Utah's Artificial Intelligence Policy Act ("UAIPA" or "the

89. *Id.* at § 183.005(b).

90. *Id*. at § 183.009.

91. *Id*. at § 183.010.

92. *Id*.

93. *Id*. at § 183.011.

94. *Id.* at § 183.011(b).

Act"), the first omnibus state law governing AI. Effective May 1, 2024, the UAIP amends the Utah Consumer Sales Practices Act and the Utah Consumer Privacy Act, and enacts the Artificial Intelligence Learning Laboratory Program to analyze, encourage, and evaluate the use of AI in the state.[95] The Act also creates a regulatory agency, the Utah Office of Artificial Intelligence Policy.[96] In contrast with Colorado's AI Act sweeping applications, Utah's AIPA is more narrowly focused on transparency in consumer interactions with generative AI. Additionally, Colorado's AI Act offers an affirmative defense for compliance with AI risk frameworks, and the UAIA has no such provision.[97] The UAIA, unlike Colorado's Act and the EU AI Act, does not mandate risk management.

The UAIA's hallmark provision is its disclosure requirement, which holds regulated occupations, including health care professionals, to a higher disclosure standard. Businesses and individuals must "clearly and conspicuously disclose" the use of AI only "if asked or prompted[.]"[98] Health care professionals and professionals in other regulated occupations must "prominently disclose" when a person is interacting with AI.

The UAIA elaborates that for health care professionals, disclosure must be provided (1) "verbally at the start of an oral exchange or conversation," and (2) through electronic messaging before a written exchange."[99] The Act does not specify the language that must be used in the disclosure, the level of detail, or whether the disclosure must be made on each communication

95. UTAH CODE ANN. § 13-72-301(2).

96. *Id.* at § 13-72-201.

97. *See* COLO. REV. STAT. ANN. § 6-1-1703(2).

98. UTAH CODE ANN. § 13-2-12(3).

99. *Id.* at § 13-2-12(5).

or may be made at the first instance of an interaction with a patient.[100]

On March 27, 2025, Utah enacted Senate Bill 226 ("SB 226), captioned "Artificial Intelligence Consumer Protection Amendments," which will come into effect May 7, 2025. SB 226 extends the UAIPA's repeal date from May of 2025 to July of 2027, and confines the disclosure requirement for regulated professionals to "high-risk" artificial intelligence.[101] "High-risk artificial intelligence interaction" is defined as an interaction involving health data, financial data, or biometric data and the provision of medical advice or mental health advice.[102]

2. Risk and Enforcement

The Utah Office of Artificial Intelligence Policy offers capped penalties and safe harbors for those who contract with the agency prior to deployment.[103]

There is no private right of action.[104] The Act provides for administrative fines of up to $2,500 per violation, and up to $5,000 for violation of an administrative or court order associated with the Act.[105] Note that if each violation of the Act is assessed on a per-instance basis, the cumulative fines could be substantial.

SB 226 explicitly adds a safe harbor to the UAIA, which states that a person will not be subject to enforcement of the UAIA's disclosure requirements if the person "clearly and

100. *Id.*

101. *Id.* at §§ 13-75-103(2), 63I-2-213(5).

102. *Id.* at § 13-75-101(5).

103. *See Office of Artificial Intelligence Policy: Regulatory Relief*, UTAH DEP'T COMM., https://ai.utah.gov/regulatory-mitigation/ (last visited May 2, 2025).

104. *See* UTAH CODE ANN. § 13-2-12.

105. *Id.* at § 13-2-12(8), (10).

conspicuously" discloses at the outset of the interaction and throughout the interaction.[106] The Division of Consumer Protection is charged with creating rules that specify the forms and methods of disclosure that satisfy the safe harbor.[107]

Although it has been a year since the enactment of the UAIA, the authors have identified no public enforcement actions.

B. Artificial Intelligence Amendments

1. The law

On March 25, 2025, Governor Spencer Cox signed into law HB 452, which governs "mental health chatbots." Effective May 7, 2025, HB 452 prohibits suppliers of "mental health chatbots" from sharing user information with third parties and prevents suppliers from using mental health chatbots to advertise products or services, unless certain conditions are met.[108] The supplier of the mental health chatbot must disclose that the chatbot is AI and not human.[109]

2. Risk and enforcement

There is no private right of action. The director of the Division of Consumer Protection may impose an administrative fine of up to $2,500 per violation, issue an injunction, order disgorgement of money received in violation of the law, and award any other relief the court determines to be "reasonable and necessary."[110] If judgment is awarded or injunctive relief is ordered, the court may impose a civil penalty of no more than $5,000 per

106. *Id.* at § 13-75-104(1).

107. *Id.*

108. *See* UTAH CODE ANN. §§ 13-72a-201, 13-72a-202.

109. *Id.* at § 13-72a-203.

110. *Id.* at 13-72a-204.

violation.[111] In such cases, reasonable attorneys' fees, courts costs, and investigation fees are mandatory.[112]

111. *Id.*

112. *Id.* at 13-72a-204(5)(a) (reflecting that "the court *shall* award the division" such fees and costs (emphasis added)).

THE SEDONA CONFERENCE COOPERATION PROCLAMATION: RESOURCES FOR THE JUDICIARY, FOURTH EDITION

Author

The Sedona Conference

Senior Editors

Ronald J. Hedges, Kenneth J. Withers

Staff Editor

Craig Morgan

Editorial Coordinators:

Joseph Bernard, Daniel McNeela

Judicial Reviewers

Hon. Helen C. Adams, Chief U.S. Magistrate Judge, Southern District of Iowa

Hon. J. Michelle Childs, U.S. Circuit Judge, D.C. Circuit

Hon. Timothy S. Driscoll, Justice, Nassau County Commercial Division, Supreme Court of New York

Hon. William F. Highberger, Superior Court of Los Angeles County, California

Hon. Karen Wells Roby, U.S. Magistrate Judge, Eastern District of Louisiana

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 12. 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, *The Sedona Conference Cooperation Proclamation: Resources for the Judiciary, Fourth Edition*, 26 SEDONA CONF. J. 513 (2025).

PREFACE

This fourth edition of *The Sedona Conference Cooperation Proclamation: Resources for the Judiciary* (the "*Resources*") continues a collaborative effort of The Sedona Conference going back fifteen years. Initial drafts of what became the public comment version of the *Resources* were presented to litigators at meetings of Working Group 1 on Electronic Document Retention and Production and to judges at programs sponsored by a variety of courts and judicial education organizations, including the Federal Judicial Center, in 2010. After publication of the first edition in 2011, an updated edition was published in 2012, followed by a second edition in 2014, before the landmark 2015 amendments to the Federal Rules of Civil Procedure went into effect.

The third edition of the *Resources* was published in 2020, in the first weeks of the COVID-19 public health crisis. Those were uncertain times for the American judicial system—both state and federal—and the nation. In-person appearances at both the trial and appellate levels were being curtailed or eliminated, and electronic communications between courts, attorneys, and parties were being encouraged or made mandatory. Nevertheless, the American judicial system continued to operate, and our judges continued to manage civil litigation. Courts adjusted to a "new normal" that challenged the traditional ways in which the bench and bar interacted to facilitate cooperation and establish mutual trust. Even more significant was the almost-universal migration of business and personal communication to the digital world. The importance of conventional paper-based documentary evidence in civil litigation diminished rapidly as email, text messages, database reports, word-processed memos, social media posts, video conferencing records and other forms of "electronically stored information" (ESI) dominated discovery and evidence. Judges need to be prepared for this continued

evolution and its consequences for the management of civil litigation.

This fourth edition of the *Resources* incorporates that experience. It assembles the most authoritative current guidance on the management of modern discovery, emphasizing practical solutions to recurring problems. The references have been carefully selected for balance and neutrality. The management strategies have been contributed by trial judges themselves, based on their personal experience. We are indebted to our Judicial Reviewers for their guidance on what advice would be most helpful to their fellow trial judges and what advice from prior editions could be updated or removed entirely. We are also indebted to our student interns, Joseph Bernard (City University of New York School of Law '25) and Daniel McNeela (Arizona State University Sandra Day O'Connor College of Law '27) for helping us understand the nuances of emerging technology, updating the numerous citations to trial and appellate court decisions, and assuring that the Internet links are current as of this publication date.

With the exception of publications of The Sedona Conference itself, no articles, forms, or other materials cited are necessarily endorsed by The Sedona Conference or the editors of the *Resources*. While we welcome those contributions, judges are reminded that civil actions call for individualized assessment of facts and law as well as independent resolution of issues. But we hope the *Resources* provides a useful overview of eDiscovery case management strategies for the generalist trial judge, as well as a refresher for the more experienced.

Kenneth J. Withers
Executive Director
The Sedona Conference
August 2025

TABLE OF CONTENTS

I. INTRODUCTION

The Sedona Conference Cooperation Proclamation: Resources for the Judiciary (the *"Resources*") is focused on the management of electronically stored information (ESI) in civil actions. A judge may have overall case management responsibility over a single action. Alternatively, a judge may be assigned to manage one or more phases or events of an action. Moreover, a judge may assign a court adjunct such as a court-appointed neutral to oversee certain phases or events. The *Resources* can assist in all these instances.

The *Resources* focuses on ESI under the Federal Rules of Civil Procedure and the Federal Rules of Evidence. These rules are comprehensive and have been interpreted and applied in many federal judicial decisions. However, the *Resources* is intended for both federal and state judges and, accordingly, looks to federal rules and decisions as exemplars of how state judges are exercising their management function. Also, bear in mind that many courts have local rules or procedures which govern ESI, and many judges have individual chambers practices that do the same.

The *Resources* recognizes that there are different models for the appropriate role of judges in civil litigation. The primary models may be characterized as "active case management" and "discovery dispute management." The first is intended to be proactive and features court supervision of pretrial activities through periodic conferences and management orders. The latter is reactive, with the court intervening in pretrial preparation only to the extent required by the rules or upon motion by the parties. The *Resources* is intended to assist judges who follow either model or a hybrid model.

Discovery as practiced in state and federal courts creates the potential for protracted disputes and the imposition of

substantial burdens on the resources of the courts and parties. The discovery of electronic information ("eDiscovery"), such as email, the content of social media, artificial intelligence, or information from databases, has multiplied those potential burdens. Active case management can prevent disputes and minimize burdens. For a discussion of the need for active case management in civil litigation, see *DCP Midstream, LP v. Anadarko Petroleum Corp.*[1] and *The Reappearing Judge*.[2]

Consequently, the *Resources* recommends active case management by judges. However, that does not mean to imply that judges should be routinely making discovery decisions for the parties. Discovery is designed to be, and remains, party driven. Active case management provides a strong framework in which the parties should develop and execute their own cooperative discovery plans. Parties are provided a clear set of expectations designed to move the evidence-gathering phase of the litigation forward in a speedy and inexpensive way, without the cost, delay, and gamesmanship associated with unmanaged discovery. The dual role of the judge under active case management is first to facilitate the cooperative formulation and execution of the discovery plan and second to intervene if the parties fail to reach an agreement or a dispute arises. Judges are reminded that civil actions call for individualized assessment of facts and law as well as independent resolution of issues. The recommendations and sample orders collected here have been selected and reviewed with the goal of encouraging the parties to cooperate in discovery to the greatest extent possible, rather than imposing judicially dictated solutions.

1. 303 P.3d 1187 (Colo. 2013).
2. S.G. Gensler & L.H. Rosenthal, 61 U. KAN. L. REV. 849 (2013).

There are "structural" reasons why a judge might follow one model and not the other. For example, in federal courts, civil actions are usually assigned to judges on an individual basis, that is, a particular civil action is assigned to one judge from commencement to conclusion. Known as "individualized case management," this model fosters active case management in the federal courts and in those state courts (or units thereof, such as dedicated business courts) that have adopted individualized management. On the other hand, many state courts, for reasons of volume and history, do not use individualized case management. Instead, from the commencement to conclusion of an action, different judges may preside over specific events (such as an initial conference, discovery dispute, motion, trial, etc.). This makes "active case management" difficult or impossible to implement, and "discovery management" may be the only workable model for judges who can only intervene after a discovery dispute has arisen.

In addition to these structural factors, there also may be a judicial philosophy that drives the adoption of a particular model by an individual judge. This philosophical question arises from consideration of whether discovery (on which the *Resources* focuses) is "party driven" as opposed to "judge driven." There are judges who, for example, follow the active case management paradigm and deem it appropriate to bring parties into court on a regular basis to work out discovery procedures and address anticipated discovery problems. It may seem counterintuitive, but many judges who adopt the active case management model report fewer disputes and reduced pressure on judicial resources, as the parties are aware that they are being closely supervised by the court. As a result, the parties may engage in more fulsome and effective communication about discovery scope and related issues. By contrast, there are other judges who believe that, given the nature of civil litigation

in our common-law tradition, parties should drive discovery and the pace of a particular action. These judges only deal with problems after they have been brought to their attention by the parties. Large caseloads also may necessitate this model of discovery management.

The amendments to the Federal Rules of Civil Procedure,[3] effective December 1, 2015, may lead federal judges toward greater involvement in the discovery process and indeed promote even more use of the active case management model. Amended Rule 1, which recognizes the need for all "actors" to strive for the "just, speedy, and inexpensive" resolution of civil litigation, suggests such involvement, as does amended Rule 26(b)(1), which emphasizes proportionality. Moreover, Rule 16(b)(3)(B)(v) authorizes a federal judge to encourage the informal resolution of discovery disputes by "direct[ing] that before moving for an order relating to discovery, the movant must request a conference with the court." How these and other amendments may affect ESI-related discovery among the states remains an open question, as does the practical application of the amendments by federal judges. Moreover, the "uneven" nature of the application of the amendments by individual federal judges is likely to continue given the limited and deferential role of appellate review of most discretionary case-management-related decisions.

Whatever the judge's role or case management philosophy, the *Resources* offers a framework for the management of ESI.

3. For the sake of brevity, the Federal Rules of Civil Procedure will not be shortened to the commonly used abbreviations "Fed. R. Civ. P." or "FRCP" when referenced in the body of the text of the *Resources*. However, they may occasionally be referred to simply "the Rules" in a broad or general context. Further, when individual rules are referenced, they will simply be referred to by their numerical indicator preceded by the word "Rule."

This edition again focuses on the "stages of litigation from the judge's perspective," starting with the preservation of ESI through the initial case management order (whatever that may be called in a specific jurisdiction), the resolution of discovery disputes, trial, and post-trial awards of costs.

To assist judges, the *Resources:*

- Articulates a clear judicial philosophy of case management and of resolution of discovery disputes;
- Identifies the stages of civil litigation when judicial management is most appropriate or desirable;
- Recognizes that not all civil actions are equal in the resources of the parties, or the actual amount in issue, and encourages proportionality;
- Identifies key issues that a judge is likely to face at each stage of litigation;
- Suggests strategies for case management or dispute resolution that encourage the parties, when possible, to reach a cooperative resolution at each stage; and
- Recommends further readings on the issues presented at each stage that have been either published by The Sedona Conference or are peer-reviewed.

The *Resources* stresses cooperation and transparency in the search for, and collection of, ESI. However, parties seldom share or negotiate search and collection methodologies, nor are they required to do so under any state or federal rule of civil procedure. Rather, when a party receives a request for production, the party and its attorney must comply with that request in a reasonable manner, and the attorney must certify that any response is made in good faith, consistent with Rule 26(g)(1). Moreover, individual judges, on an ad hoc basis or pursuant to local rule

or individual procedure, may require some level of cooperation in the search for and collection of ESI.

Note that issues that commonly arise in eDiscovery are posed throughout the *Resources*, without definitive "one size fits all" solutions. We cannot offer definitive answers to every question related to case management. The answer to a particular problem in any individual case will depend on the facts and the arguments presented by the parties. But the *Resources* provide practical examples of how trial judges have successfully addressed these issues in their cases. These examples can act as a roadmap or compass and can help "lead the way forward."

The *Resources* is not intended to be authoritative and should not be cited as such. Rather, it identifies issues that federal and state judges may confront in the management of civil actions that involve ESI and suggests strategies that judges might employ. The *Resources* also provides, in some instances, sample forms or orders that illustrate approaches taken by individual judges in specific actions. In addition, the *Resources* includes non-exhaustive references to written materials that judges may wish to consult. And while the publications of The Sedona Conference represent broad, general consensus among The Sedona Conference Working Group Series members, neither those publications nor the supplementary materials referenced in the *Resources* necessarily represented the views of the authors and editors of this publication.

II. REVIEW OF EXISTING LITERATURE ON EDISCOVERY FOR JUDGES

1. The *Resources* assumes that the judicial reader is familiar with eDiscovery in general—including the differences between eDiscovery and paper discovery, the problems arising out of the volume, variety, complexity, and cost associated with eDiscovery, and the recurring issues of accessibility, form of production, and waiver of attorney-client privilege or work-product protection.

2. For judges who are unfamiliar with eDiscovery, or who may wish to become reacquainted with it, several publications provide overviews that are unbiased, peer-reviewed, and well-suited. Any judge who presides over, or who anticipates presiding over, civil litigation involving eDiscovery is encouraged to be familiar with the following, each of which was the product of collaborative study and consensus:

   2.1 Selected Recent Sedona Conference Working Group Series Publications (August 2025). This Sedona document summarizes various publications, including those listed below and elsewhere in these Resources.

   2.2 *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production (Oct. 2017).* The third edition of *The Sedona Principles* represents the culmination of a process by which judges, practicing attorneys, and academics considered developments in eDiscovery practice over the past decade, incorporating the 2015 amendments to the Federal Rules of Civil Procedure. Considered to be an authoritative text on eDiscovery, *The Sedona*

Principles provides a lens through which eDiscovery can be managed.

2.3 The Federal Rules of Civil Procedure and, in particular, the often-overlooked Advisory Committee Notes to the 2006 and 2015 amendments to Rules 1, 16, 26, and 37 cited in these *Resources*. While the *Resources* does not urge the adoption of the Federal Rules of Civil Procedure in any state, it does suggest that the federal rules provide both the outline of a judicial management philosophy and practical suggestions for state judges as they deal with eDiscovery.

2.4 R.J. Hedges, B.J. Rothstein & E.C. Wiggins, *Managing Discovery of Electronic Information, Third Edition (FJC: 2017)*. "This third edition of the pocket guide on managing the discovery of electronically stored information (ESI) covers the December 1, 2015, amendments to the Federal Rules of Civil Procedure and reflects the rise of new sources of ESI, particularly social media, and updates judges on how ESI may be searched. It also suggests case-management techniques that judges might use in smaller civil actions in which the costs of ESI discovery could hamper resolution on the merits."

2.5 *Civil Litigation Management Manual, Third Ed. (U.S. Courts 2022)*."This manual provides trial judges a handbook on managing civil cases. It sets out a wide array of case-management techniques, beginning with early case screening and concluding with steps for streamlining trials and final disposition. It also discusses a number of special topics, including pro se and high visibility cases, the role of staff, and automated programs that support case management."

3. All of the above are "general" publications about eDiscovery. There are, of course, other publications that address specific issues in discovery such as preservation, non-party discovery, and admissibility. States may have their own primers as well, and state court judges are encouraged to review materials that are unique to their state. Further readings appear throughout the "Stages of Litigation from a Judge's Perspective" section of *The Resources*. These readings are primarily publications of The Sedona Conference.

   3.1 *See, e.g.*, *Bench Book for New York State Judges Pertaining To The Discovery Of Electronically Stored Information ("ESI")* (November 2020 Edition).

   3.2 *See also*, *2019 Florida Handbook on Civil Discovery Practice*, Chapter 3 (pgs. 10-54).

III. GENERAL RECOMMENDATIONS FOR JUDGES

1. A review of the literature cited in Section II reveals a common thread: The key to reducing cost and delay that may be associated with eDiscovery is judicial attention to discovery issues and case management starting early and continuing through every stage of an action. The expenditure of a small measure of judicial resources at the beginning of litigation to set the tone and direction of eDiscovery—and a judge's later availability at each stage of the action—will likely save the expenditure of significantly more judicial resources later.

2. With the above in mind, the *Resources* makes the following recommendations:

   2.1 To the extent possible and consistent with their duties and calendars, judges should establish a hands-on approach to case management early in each action. The scheduling conference may be a good place to start this discussion and set expectations.

   2.2 Judges should establish deadlines and keep parties to those deadlines (or make reasonable adjustments as needed) with periodic reports from parties or conferences.

   2.3 Judges should demand attorney competence, which includes knowledge of their clients' relevant records and communications, and the ways they use information technology.[4]

---

4. *See* State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2015-193, available at

2.4 Judges should encourage parties to meet before discovery commences to develop realistic discovery plans and to anticipate discovery related issues that may arise. Judges also should encourage counsel to communicate with each other and the court frequently and candidly about the status of discovery.

2.5 Judges should encourage parties to consider proportionality, balancing the needs of the case with the potential cost and burdens of discovery, when making demands for preservation and in discovery-related requests and responses.[5]

2.6 Judges should exercise their discretion to limit arguably disproportionate discovery through appropriate protective orders, phased or prioritized discovery, cost shifting, or other mechanisms.

2.7 If necessary, judges should exercise their authority to award sanctions under relevant statutes or rules or as an exercise of their inherent authority against parties and/or counsel who create unreasonable cost or delay, or who otherwise frustrate the goals of Rule 1 or its state equivalents.

---

https://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/CAL%202015-193%20%5B11-0004%5D%20(06-30-15)%20-%20FINAL1.pdf.

5. *See* Federal Rule of Civil Procedure 26(b)(1) and accompanying Advisory Committee Notes to the 2015 Amendments; *see also* Grimm, Paul W., "Are We Insane? The Quest for Proportionality in the Discovery Rules of the Federal Rules of Civil Procedure" (2016) (unpublished LL.M. thesis, Duke University School of Law), available at https://scholarship.law.duke.edu/mjs/13.

3. These broad recommendations should not be interpreted to suggest that judges should issue blanket orders that dictate the scope of discovery, the nature of party discovery requests or responses, the form or forms of production, or any other details of the conduct of discovery. Our civil litigation system does not contemplate that a judge conducts discovery, and eDiscovery in particular is fraught with highly technical and case-specific issues that are best left to the parties to resolve. Moreover, the recommendations transcend specific rules of civil procedure that may be in effect in a specific jurisdiction. The recommendations can be applied equally in federal or state litigation, and in every court or proceeding in which discovery is allowed, from family to complex commercial courts.

4. The recommendations are made with the understanding that there may be circumstances that require a judge to bring pressure to bear on parties and attorneys who, left to their own devices, might increase the burden and cost of an action.

5. The recommendation above that "judges should demand attorney competence" merits some extended discussion. Attorneys, for the most part, are generalists. Some focus on particular areas of the law. However, in whatever area they might practice, attorneys (as a general proposition) are not experts in the technologies that can be encountered in eDiscovery. For example, attorneys should not be expected to develop mechanisms for, or conduct, automated searches of data.

    5.1 What is expected of attorneys is competence within the meaning of ABA Model Rule of Professional Conduct 1.1, Comment 8. For example, an attorney should

understand how to reasonably protect client confidences when communicating electronically. An attorney should also understand when he needs the assistance of an eDiscovery specialist or consultant. These are not simply matters of ethics: Attorney incompetence in eDiscovery can lead to the waste of party and court resources and frustrate the "just, speedy, and inexpensive determination of every action and proceeding."[6]

6. In addition to the recommendations, judges may wish to consider whether to appoint a court-appointed neutral under Rule 53 or its state equivalents to address ESI-related issues in specific actions when the expense of a court-appointed neutral might be justified, and subject to local rules and practice. Plainly, the appointment of a court-appointed neutral should be a rare event. However, given a significant volume of ESI in issue, a court-appointed neutral might assist a court in, for example, undertaking the *in camera* review of ESI alleged to be non-discoverable because of attorney-client privilege protection of work product, trade secret, private, or otherwise confidential.

   As an alternative to the appointment of a court-appointed neutral, judges might consider, if appropriate and authorized by rule or order, the appointment of an eDiscovery mediator to assist the parties in reaching the amicable

---

6. FED. R. CIV. P. 1. For a discussion of competence, see, e.g., R.J. Hedges & A.W. Walker, Competence with Electronically Stored Information: What Does It Currently Mean in the Context of Litigation and How Can Attorneys Achieve It?, 16 DDEE 322 (2016), available at https://news.bloomberglaw.com/e-discovery-and-legal-tech/insight-discovering-artificial-intelligence?context=search&index=1.

resolution of their ESI-related disputes.

7. The recommendations apply to all civil actions and proceedings, but with the understanding that "large" or complex litigation might particularly need active case management. *Nonetheless, they are essential to eDiscovery that takes place in "small" actions or, in other words, the vast majority of litigation in our civil litigation system*. Judges should take care to utilize all the tools available to them to limit ESI-related costs such that those costs are not disproportionate to the value of any particular small action.[7]

8. The next section of the *Resources*, "The Stages of Litigation from a Judge's Perspective," analyzes the steps in the litigation process at which judicial action is likely to be necessary and desirable. Each stage presents key issues a judge is likely to confront, suggests possible strategies for the management of those issues, identifies representative decisions and sample orders, and suggests further reading for those who wish to learn more.

7. *See* The Sedona Conference, *Primer on Managing Electronic Discovery in Small Cases*, 24 SEDONA CONF. J. 93 (2023.

IV. THE STAGES OF LITIGATION FROM A JUDGE'S PERSPECTIVE

1. Preservation

1.1 Preservation of relevant ESI is the key to eDiscovery. Absent preservation, meaningful discovery cannot be conducted. Indeed, absent preservation, a judge may be faced with the task of determining whether to impose sanctions for the loss of ESI ("spoliation") and what those sanctions should be. Nevertheless, preservation decisions are usually made before the parties see a judge for the first time and often before litigation commences. Preservation decisions also implicate questions of attorney-client privilege and work-product protection. Thus, a judge should be prepared to address preservation issues as early as possible in the action.

1.1.1 Preservation is a subject that must be considered by the parties at the Rule 26(f) conference. Rule 26(f)(3)(C). Scheduling orders issued pursuant to Rule 16(b)(3)(B)(iii) also may address preservation. These Rules allow federal judges to address issues of "timing" and scope of preservation soon after a responsive pleading is filed.

1.1.2 State judges may not have the benefit of rules equivalent to Rules 26(f) or 16(b) in terms of addressing ESI specifically. Case law may, however, provide similar principles. In any event, state judges should strive for early identification and resolution of any preservation-related disputes.

1.2 Issues presented

1.2.1 Significant preservation decisions may be made before formal litigation begins, and thus before the judge has any opportunity to manage the case. Generally speaking, the duty to preserve arises when a party knows of litigation or when litigation is reasonably foreseeable. Presumably, a putative plaintiff must begin to preserve at some point before the filing of a complaint. Similarly, a defendant may be aware that it will be involved in litigation before service of process. If so, the defendant must preserve at the earlier date. The *trigger* for the existence of a duty to preserve is fact-sensitive and often in dispute. It should be noted that preservation for the purposes of litigation may conflict with information governance policies, which, among other things, call for the routine and automatic deletion of data. Moreover, preservation may conflict with data privacy laws such as the California Consumer Privacy Act, the Illinois Biometric Information Privacy Act, and the New York SHIELD Act, all of which provide for, among other things, "rectification" and "minimization" of protected data.

1.2.2 There is no realistic mechanism for judicial determination of the existence or scope of a duty to preserve before litigation commences. There may be significant costs involved in preservation, especially if a party, in the absence of any judicial direction, believes it must *over-preserve*

discoverable information. This may lead to disputes between parties that will require judicial resolution at an early stage.[8]

1.2.3 The decision to preserve and the scope of preservation are questions that attorneys should address with their clients. That advice, as well as the communication of that duty (to, for example, employees and third-party contractors), is presumably subject to attorney-client privilege and work-product protection. Disputes pertaining to the nature of communications involving privilege—and the scope of any privilege or work product—frequently arise.

1.2.4 It should be emphasized that the scope of the duty to preserve may be broader than the scope of discovery. This is particularly so in the federal courts (and state equivalents) given the limitation of discovery, since the 2015 amendments, to information that is relevant to claims and defenses under Rule 26(b)(1).

1.3 Suggested judicial management strategies

1.3.1 Require by local rule that the parties discuss preservation at the initial conference between

8. Often, the court is only involved in preservation decisions after-the-fact, when considering a motion for sanctions for the failure to preserve discoverable information. Federal Rule of Civil Procedure 37(e), adopted in 2015, was designed to reduce over-preservation by limiting sanctions if the loss of discovery ESI was inadvertent or did not result in prejudice to the requesting party.

the parties as required by Rule 26(f) or its state equivalents.

1.3.2 Direct the parties to present any disputes about preservation to the court as soon as possible so that the judge can issue appropriate orders regarding what should or should not be preserved in the earliest stage of litigation. This may be a topic to discuss with the parties at the initial Rule 16(b) conference.

1.4 Representative decisions

1.4.1 *4DD Holdings, LLC v. United States*, 143 Fed. Cl. 118 (Fed. Cl. 2019) (government's failure to issue legal hold for three months after "trigger").

1.4.2 *Culhane v. Wal-Mart Supercenter*, 364 F. Supp. 3d 768 (E.D. Mich. 2019) (risk manager's failure to follow legal hold procedures).

1.4.3 *Herzig v. Arkansas Found. for Med. Care Inc.*, No. 2:18-cv-02101, 2019 WL 2870106 (W.D. Ark. July 3, 2019) (plaintiffs' use of ephemeral messaging after duty to preserve attached).

1.4.4 *Schmidt v. Shifflett*, CIV 18-0663 KBM/LF, 2019 WL 5550067 (D.N.M. Oct. 28, 2019) (finding duty to preserve defendant truck driver's cell phone and its data arose when nature of accident put defendants on notice of a claim in reasonably foreseeable litigation or, at the latest, on receipt of preservation demand from plaintiff's attorney).

1.4.5 *Goodale v. Elavon, Inc.*, No. 23-5013, 2023 WL 9111441 (6th Cir. Dec. 12, 2023) (rejecting, among other things, argument that duty to preserve triggered by plaintiff's call to defendant's ethics hotline because it did not "contain any mention of potential age discrimination or litigation").

1.4.6: *Chepilko v. Henry*, 722 F. Supp. 3d 329 (S.D.N.Y. 2025) (denying motion for sanctions for loss of video footage because defendants had no duty to preserve).

1.5 Further reading

1.5.1 The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341 (2019).

1.5.2 Rule 37(g)(1)(B)(1)(A), Rules of Civil Procedure for the Superior Courts of Arizona ("A party or person has a duty to take reasonable steps to preserve electronically stored information relevant to an action once it commences the action, once it learns that it is a party to the action, or once it reasonably anticipates the action's commencement, whichever occurs first. A court order or statute also may impose a duty to preserve certain information.").

1.5.3 Rule 37(g)(1)(B), Rules of Civil Procedure for the Superior Courts of Arizona ("A person reasonably anticipates an action's commencement if: (i) it knows or reasonably should know that it is likely to be a defendant in a specific action; or (ii)

it seriously contemplates commencing an action or takes specific steps to do so.").

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

2. Parties' early case assessment

2.1 Early case assessment ideally takes place *prior* to joinder of issue. That assessment is a process by which a party undertakes an internal cost-benefit analysis to determine whether to settle or litigate. This process is nothing new. What is new, however, is the need to consider the preservation, collection, review, and production of ESI in making that assessment.

2.2 Early case assessment, although included here as a *marker* in the litigation process, is not a stage of litigation from a judge's perspective, but it can lead to a better-informed and more effective Rule 26(f) conference and initial case management order under Rule 16(c)(2).

2.3 Because early case assessment does not involve the judge, there are no "issues presented," "suggested judicial management strategies," "sample orders," or "further reading" presented here.

2.4 The results of an early case assessment in a particular action are likely to be protected from discovery by attorney-client privilege or work-product protection. Nevertheless, undertaking the cost-benefit analysis necessary for any assessment is an important step from a party's perspective, and the knowledge that one was

performed by a party may inform the judge of the likelihood of early settlement.

2.5 National Center for State Courts, Coronavirus and the Courts, (last visited Feb. 9, 2022). This website collects orders, protocols, bench books, and other resources addressing court operations during the pandemic from state courts nationwide.

2.6 U.S. Courts, Court Orders and Updates During COVID-19 Pandemic, (last visited Feb. 9, 2022). This website collects court orders and memoranda addressing court operations during the pandemic from federal courts nationwide.

2.7 S.A. Thumma, *A Virtual Step Forward: Remote Court Hearings in Response to the Pandemic*, ASU MORRISON INST. FOR PUB. POLICY (2021). This monograph summarizes the "Post-Pandemic Recommendations" of an emergency workgroup of the Arizona Supreme Court, available at https://scholar.smu.edu/cgi/viewcontent.cgi?article=1039&context=smulrforum.

2.8 Consider using artificial intelligence or GenAI tools to conduct or have conducted preliminary research on issues that might be before judges. In this regard, see Judge Newsom's concurrence in Snell v. United Specialty Ins. Co., 102 F.4th 1208 (11th Cir. 2024)., and the majority, concurrence and dissent in Ross v. United States, 331 A.3d 220 (D.C. 2025). In doing so, be aware of the possible limitations of the tool and the need to verify the product of its use. In this regard, see Judge Newsom's concurrence:

In his most recent year-end report on the state of the federal judiciary, Chief Justice Roberts cautioned that the "use of AI requires caution and humility." Roberts, supra, at 5. I wholeheartedly agree. Importantly, though, I also agree with what I take to be the report's assumption that AI is here to stay. Now, it seems to me, is the time to figure out how to use it profitably and responsibly. It's in that spirit that I've offered these preliminary thoughts about whether and how LLMs might aid lawyers and judges in the interpretive enterprise. Plenty of questions remain and I'm sure I haven't even identified all of them. But—and this is my bottom line—I think that LLMs have promise. At the very least, it no longer strikes me as ridiculous to think that an LLM like ChatGPT might have something useful to say about the common, everyday meaning of the words and phrases used in legal texts.

In this regard, judges should be aware of their ethical obligations when using generative AI. See W.K. McGill, *Ethical Rules to Consider When Using Generative Artificial Intelligence as a Judge*, Vol. 27, Issue 3, JUDICIAL DIV. RECORD (ABA: Apr. 23, 2024).

See also M.L. Greenstein, *Judges May Have a Duty to Maintain Literacy in 'Tech Talk,'* Vol. 63, No. 1, JUDGES' JOURNAL 40 (ABA: Winter 2024).

In conclusion, recall the comments of Chief Justice Roberts in the 2023 Year-End Report on the Federal Judiciary (Dec. 31, 2023):

"Rule 1 of the Federal Rules of Civil Procedure directs the parties and the courts to seek the 'just, speedy, and inexpensive' resolution of cases. Many AI applications indisputably assist the judicial system in advancing those goals. As AI evolves, courts will need to consider its proper uses in litigation. In the federal courts, several Judicial Conference Committees—including those dealing with court administration and case management,

cybersecurity, and the rules of practice and procedure, to name just a few—will be involved in that effort.

"I am glad that they will be. I predict that human judges will be around for a while. But with equal confidence I predict that judicial work—particularly at the trial level—will be significantly affected by AI. Those changes will involve not only how judges go about doing their job, but also how they understand the role that AI plays in the cases that come before them."

2.9 E.C. Wiggins, *Remote Participation in Bankruptcy Court Proceedings*, FEDERAL JUDICIAL CENTER (2017). This guide was released before the pandemic. It is intended to provide an overview of "distance participation" and, among other things, "encourage the use of DP technology so as to promote access to the courts, make the best use of existing judicial re-sources, and contain costs."

2.10 Brooke Meyer & Natalie Anne Knowlton, *IAALS' Comment to the Michigan Supreme Court on Virtual Proceedings and Lessons Learned from the Pandemic*, INSTITUTE FOR THE ADVANCEMENT OF THE AMERICAN LEGAL SYSTEM (Nov. 15, 2021).

These comments, in response to the preliminary findings, best practices, and recommendations from the Michigan State Court Administrative Office, collects and draws on the experiences of various state courts to suggest "the importance of retaining some of the virtual proceeding processes in place during the pandemic.

2.11 New Jersey Supreme Court, Notice to the Bar and Public, Future of Court Operations—Continuation of Both In-Person and Virtual Court Operations (Nov. 18, 2021).

2.12 U.S. District Court for the District of New Jersey, Standing Order 2021-11, In re: Court Operations Under the Exigent Circumstances Created by COVID-19 (Dec. 29, 2021).

2.13 Judicial Branch of California, California Courts Newsroom, Judicial Branch Emergency Actions, (last visited Feb. 5, 2022).

2.14 Supreme Court of Texas, Forty-Seventh Emergency Order Regarding the COVID-19 State of Disaster, Misc. Docket No. 22-9005.

2.15 New York State Unified Court System, Coronavirus and the New York State Courts, (last visited Feb. 5, 2022).

2.16 California Rules of Court, Rule of Court 3.672 Remote Proceedings (effective Jan. 1, 2022).

2.17 CAL. CIV. PROC. CODE § 367.75 - Parties appearing remotely; conducting conferences, hearings and proceedings (effective Jan. 1, 2022).

3. Initial scheduling order

3.1 Rule 16(a) provides that, "the court may order the attorneys and any unrepresented parties to appear for one or more pretrial conferences" for various purposes. There may be state equivalents to Rule 16(a) and, absent one, a state judge might, if within his authority, direct that a conference be conducted. An initial scheduling conference furthers the guiding principle in Rule 1 that requires the Rules be "construed, administered, and employed by the court and the parties to secure the

just, speedy, and inexpensive determination of every action and proceeding."

3.1.1 The Rule 16(a) order directs attorneys and *pro se* litigants to appear before a judge to establish, among other things, "early and continuing control so the case will not be protracted because of lack of management."[9] This initial order is an opportunity for the judge to communicate the court's expectation that attorneys and parties will meaningfully prepare for the Rule 26(f) conference and the first Rule 16(b) conference. It may also serve to remind parties and counsel that sanctions may be imposed under Rule 16(f)(1)(B) if they are "substantially unprepared to participate." The initial order is also an opportunity for the judge to communicate the court's expectation of how the parties should strive to cooperate in discovery.

3.2 Issues presented

3.2.1 One of the major problems that judges face is the parties' lack of preparation for the first conference with the judge. Rule 26(f) describes when parties should have their first conference. It also describes the required topics for parties to discuss at the conference and how the results of that conference should be presented to the judge. In federal courts, local rules and chambers

9. FED. R. CIV. P. 16(a)(2).

practices may supplement the list of factors to be discussed under Rule 26(f).

3.2.2 Several states have adopted statutes, rules, or orders that function in much the same way as Rule 26(f). In state courts where there is no equivalent to Rule 26(f), it might be useful for the judge presiding over a particular action to direct the parties to confer before the initial conference with the judge, discuss eDiscovery issues, and report to the court. This would, at the least, compel the parties to consider the issues suggested by Rule 26(f) and enable the parties to avoid conducting eDiscovery in a vacuum. However, the rules of certain states may place limits on what courts may impose on parties, as in *Antero Resources v. Strudley*,[10] which held that a "modified" case management order that required a plaintiff to establish *prima facie* evidence in support of a claim before obtaining discovery was not authorized under Colorado law.

3.2.3 The pandemic led to what is likely to be a fundamental shift in how discovery and judicial proceedings will be conducted. Rather than in-person depositions and case-management related events, remote and hybrid ones should be planned for by parties and judges. The Initial Scheduling Order offers judges the opportunity to remind attorneys and parties that they should consider what discovery or case management

10. 2015 CO 26 (Colo. 2015).

events might take place other than on an in-person basis, discuss this topic during the Rule 26(f) conference, and be prepared to address it at the first Rule 16(b) conference. Reference might be made to Rule 30(b)(4)—or its state equivalent—which allows for remote depositions by stipulation or order in the event of a dispute.

3.3 Suggested judicial management strategies

3.3.1 Require the parties to confer on eDiscovery and any other topic enumerated in Rule 26(f) and local rules before the initial case management conference. This should impress on the parties the intent of the court that the parties and their counsel take their obligations to confer seriously and that the court will frown upon any failure to do so.

3.3.2 Remind the parties that, under Rule 26(d)(2)(A), parties may deliver discovery requests under Rule 34 that will be "considered to have been served at the first Rule 26(f) conference" under Rule 26(d)(2)(B). This will allow the parties to raise objections to the requests and arrive at agreements pertaining to the delivered requests. Both disputes and agreements can then be presented at the initial case management conference.

3.3.3 Suggest that each party identify a person or persons particularly knowledgeable about the party's electronic information systems and who

is prepared to assist counsel in the Rule 26(f) conference and later in the litigation.

3.3.4 Encourage the parties to consider any issues of privilege, trade secret and confidentiality, the inadvertent disclosure of privileged information, and the form and timing of privilege logs. Refer the parties to Federal Rule of Evidence 502 (discussed in Section IV.12.2.5 and 12.2.6) or its state equivalents, as they may not be familiar with it.

3.3.5 Encourage the parties to identify whether discovery will be needed from non-parties, the scope of proposed non-party discovery, and an appropriate allocation of costs.

3.3.6 Remind the parties that consistent with the goals of Rule 1, their best interests and those of the court might be served by remote or hybrid depositions rather than in-person ones. In doing so, the parties should be reminded of the formalities required by Rules 28 and 30 that must be adhered to so that the deposition and documents identified at it might be used in subsequent proceedings, including trials. During the pandemic, many court reporting services developed expertise in virtual depositions, often hosting the video platform and giving lawyers tips on how to effectively handle documents and create the video record.

3.3.7 Encourage the parties to consider staged, sequenced, or phased discovery, where doing so is

likely to reduce costs by narrowing the scope of discovery as the litigation progresses.

3.3.8 Direct the parties to report on any agreements reached or disagreements encountered at the Rule 26(f) conference as well as any disagreements and stipulations under Rule 29 or state equivalents.

3.3.9 Consider whether, given the nature of a particular dispute, the resources of the parties, and the rules of the jurisdiction, referral to a Magistrate Judge, appointment of a court-appointed neutral, or appointment of a discovery mediator would be appropriate.

3.4 Sample orders

3.4.1 New York State Unified Court System, Part 202: Uniform Civil Rules for the Supreme Court and the County Court, Section 202.70: Rules of the Commercial Division of the Supreme Court.

3.4.2 Standing Orders, Hon. William Alsup, United States District Court for the Northern District of California, Supplemental Order to Order Setting Initial Case Management Conference Before Judge William Alsup (providing guidance on "recurring practical questions that arise prior to trial and . . . [imposing] certain requirements for the conduct of the case").

3.4.3 New York State Uniform Rules for the Supreme and County Courts (Rules of Practice for the

Commercial Division), Rule 36 (effective Dec. 13, 2021), allowing video technology for evidentiary hearings or non-jury trials, provided that the "technology must enable:

> i. a party and the party's counsel to communicate confidentially;
>
> ii. documents, photos, and other things that are delivered to the court to be delivered to the remote participants;
>
> iii. interpretation for a person of limited English proficiency;
>
> iv. a verbatim record of the trial; and
>
> v. public access to remote proceedings."

3.4.4 *State v. Biden*, Civil Action No. 3:21-CV-065 (S.D. Tex. July 28, 2021) (setting forth "basic instruction on how to use Zoom" for virtual initial and other pretrial conferences and including this note: "you are NOT required to wear formal courtroom attire during the videoconference. You are, however, required to wear clothes.")

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

4. The conference between parties to formulate a discovery plan

4.1 The conference itself

4.1.1. The initial conference between parties contemplated by Rule 26(f) is central to the management of eDiscovery (indeed, all discovery). If done correctly, this conference will enable the parties to establish, on a cooperative basis, how the action will proceed and will reduce the cost of eDiscovery and any delay associated with the resolution of discovery disputes. The discovery plan should guide the issuance of the initial case management order.

4.1.2 Judicial management of the conference itself should be minimal once the court establishes the expectations and the agenda. The conference is driven by the *parties*—not the *judge*. Indeed, the judge need not even be aware that a conference took place until a discovery plan is submitted.

4.1.3 The conference contemplated by Rule 26(f) is not a perfunctory or "drive-by" requirement. Depending on the nature of the particular action and the volumes and varieties of discoverable ESI from multiple sources, the conference may require several meetings, in person or through remote access, and may involve representatives of corporate parties such as information management personnel and retained consultants. Judges should be mindful of the need for multiple meetings and consider extending deadlines for submission of a discovery plan, because these meetings might lead to agreements that would avoid or minimize discovery disputes to the benefit of judges and parties.

4.2 Issues presented

4.2.1 There may be instances where the conference does not in fact take place or, if it does, where the conference was not *meaningful.*

4.2.2 To be useful for the issuance of an initial scheduling order, a comprehensive discovery plan should be submitted to the judge.

4.3 Suggested judicial management strategies

4.3.1 Discourage use of perfunctory or "drive-by" conferences by the parties. You may need to describe the court's expectations as to what an appropriate "meet and confer" would look like.

4.3.2 Develop, with the concurrence of colleagues, a form of discovery plan that supplements Rule 26(f) and incorporates any additional topics identified in local rules or chambers practices and sets forth the advice contemplated below.

4.3.3 Advise the parties that the court will be available by email, telephone, Zoom, or letter to resolve disputes that might arise in the Rule 26(f) process and remind the parties of the availability of informal or expedited resolution of discovery disputes pursuant to Rule 16(b)(3)(B)(v).

4.3.4 Suggest that involvement of knowledgeable party representatives or experts may be beneficial in addressing ESI-related topics, with appropriate stipulations regarding any statements made by them.

4.3.5 Advise that, at least in complex actions with likely discovery issues or large volumes of ESI, the conference may be a continuing process requiring multiple meetings. This may require that appropriate time be afforded to the parties before a discovery plan is submitted, a case management conference conducted, or an initial case management order entered.

4.3.6 Remind that parties that, consistent with 3.3.6 above, it might be appropriate to conduct depositions on a remote basis and that, when appropriate, the court will allow judicial proceedings such as status conferences or discovery disputes to occur on a remote or hybrid basis.

4.4 Sample orders

4.4.1. United States District Court for the Western District of Pennsylvania, Local Civil Rule 26.2, Discovery of Electronically Stored Information (addressing party obligations in preparation for and with regard to Rule 26(f) conference).

4.4.2. United States District Court for the Western District of Washington, Redline [Model] Agreement re: Discovery of Electronically Stored Information (addressing, among other things, scope of preservation).

4.4.3 Procedures, Hon. Lee H. Rosenthal, United States District Court for the Southern District of Texas, The Parties' Rule 26(f) Meeting (addressing topics parties are to discuss).

4.5 Further reading

4.5.1 Ariana Tadler, et al, *The Sedona Conference "Jumpstart Outline"* (Mar. 2016).

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

5. Case management order

5.1 Rule 16(b)(1) directs federal judges to issue case management orders after the parties have engaged in the Rule 26(f) process and submitted a discovery plan. State judges, of course, are not bound by the Federal Rules of Civil Procedure. Nevertheless, the topics that Rule 16(c)(2) sets out for a federal judge to contemplate in an initial case management order suggest a useful framework for state judges to look to as they meet with parties for the first time.

5.2 Issues presented

5.2.1 There may be times when parties have not conferred before their first meeting with the judge, either in violation of Rule 26(f), a state equivalent, or a judicial direction to confer. The judge will then be faced with the option of sending the parties off for a limited conference or proceeding to enter a case management order without the benefit of a plan.

5.2.2 Assuming that parties have reached agreement on one or more questions of fact or legal issues, the agreement should be incorporated in some

way into case management. However, a judge presumably may need to exercise her discretion to incorporate party agreements into case management needs consistent with the goals of Rule 1.

5.2.3 The judge should consider when to schedule subsequent conferences with the parties. This might require flexibility in scheduling by the judge. For example, the judge might set a firm date. Alternatively, if the judge sequences discovery, she might schedule periodic conferences after a particular phase of discovery has been concluded.

5.3 Suggested judicial management strategies

5.3.1 Incorporate, as appropriate, party agreements in the initial case management order.

5.3.2 Resolve any disagreements as soon as practicable, perhaps at the case management conference itself.

5.3.3 Announce the judge's availability in between scheduled conferences upon presentation of a letter/email from the aggrieved party, or (preferably) a jointly prepared letter.

5.3.4 Schedule a further conference or conferences as needed in the initial case management order. Alternatively, given the complexity of a particular case, direct the parties to check in telephonically on a regular basis (perhaps biweekly or

monthly) to monitor progress and apprise of pending or anticipated disputes.

5.3.5 Suggest that rather than directed interrogatories or Rule 30(b)(6) depositions, the parties informally exchange information about their respective electronic information systems.

5.4 Representative decisions

5.4.1 *P&B Franchise, LLC v. Dawson*, No. CV-23-00784-PHX-SMB, 2024 WL 426956 (D. Ariz. Jan. 29, 2024) (ordering parties to meet and confer "to propose a protocol" for ESI sought by plaintiffs)

5.5 Further reading

5.5.1 Managing Discovery of ESI (FJC 3d Ed. 2017).

5.5.2 The Sedona Conference, *The Sedona Conference Primer on Managing Electronic Discovery in Small Cases*, 24 SEDONA CONF. J. 93 (2023).

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

6. Scope of discovery

6.1 Defining the scope of eDiscovery

6.1.1 All discovery in the federal courts is governed by Rule 26(b)(1), which provides that "[p]arties may obtain discovery regarding any nonprivileged matter that is *relevant* to any party's claim

or defense and proportional to the needs of the case . . . "

6.1.2 The 2015 amendment eliminated the expansive "subject matter" language of the pre-2015 version of the rule but provides that "[i]nformation within this scope of discovery need not be admissible in evidence to be discoverable."

6.1.3 Rule 26(b)(1) stresses proportionality in discovery. The factors are:

- importance of the issues at stake in the action;
- amount in controversy;
- parties' relative access to relevant information;
- resources of the parties; and
- importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.

6.1.4 The scope of discovery may be different under state rules, at least some of which adopted the text of Rule 26(b)(1) before it was amended in 2015. Moreover, states may take different approaches to discovery, such as the Utah Rule of Civil Procedure 26(b), which expands on the text of Federal Rule 26(b).

6.2 Issues presented

6.2.1 Requests for discovery of ESI often lack a clear connection to the issues in the action. For example, parties may seek "all email" or "all databases" from an opposing party. Such requests

may be acceptable if directed to a narrowly defined event, communication, or issue but would not be acceptable without such limitation(s). In the first instance, the scope of eDiscovery should be defined by the parties (within the confines of Rule 26(b)(1)) with reference to claims and defenses set forth in the pleadings. However, in state court actions, the parties may request, and the court may consider, broader *subject-matter* discovery for good cause, assuming such states allow subject-matter discovery. Since one or both parties may desire broader discovery or may be unsure as to what the appropriate scope of discovery should be, the court should require that the parties negotiate the scope of discovery pursuant to Rule 26(b)(1) and attempt to reach agreement at the outset. The scope may later be modified by agreement or by court order.

6.2.2 There will always be new sources of ESI that will be relevant to litigation pending before a judge. Of particular concern for judges is the rise of social media, both in terms of simple volume, near-universal access and use, and its potential as a source of discoverable ESI. Discovery of social media can be extensive and can implicate the privacy interests of parties and non-parties who participate on social media platforms. If agreement cannot be reached, there is no consensus as to how social media discovery should be conducted.

6.2.2.1 The discovery of social media should be governed by the same principles that govern discovery of other electronically stored information. While many social media platforms provide options to restrict public access to individual postings or whole accounts, such "privacy settings" do not shield relevant, non-privileged ESI from discovery.

6.2.2.2 Discovery of particular social media platforms, or of particular applications supported by those platforms, may be subject to, and limited by, the Stored Communications Act.[11] Discovery of social_media may also require a judge to review terms of service to determine what content a party or subpoenaed non-party can retrieve from a social media provider. There may also be circumstances when a judge will be required to conduct an *in camera* review because of privacy concerns and when a party will require the assistance of a retained consultant to retrieve content.

6.2.3 There may be instances where a party in a civil action seeks to engage in so-called transnational discovery, that is, discovery of ESI that is located in another country and subject to the possession, custody, or control of an adversary party. In that

11. 18 U.S.C.A. § 2701 *et. seq.*

circumstance, production of ESI may be alleged by the producing party to be "exempt" from discovery because of a data privacy law such as the General Data Protection Regulation (GDPR) of the European Union or a commercial blocking statute of the host country.

6.3 Suggested judicial management strategies

6.3.1 Require that the discovery plan address the scope of eDiscovery and describe any disputes as to scope.

6.3.2 Require any party seeking discovery into matters beyond claims and defenses to explain why the proposed broader discovery is necessary and relevant to the needs of the case.

6.3.3 Resolve any disputes as to scope in the initial case management order, if possible; otherwise, at the time a dispute arises.

6.3.4 Require the parties to focus any requests for discovery of social media to relevant and necessary ESI.

6.3.5 Tailor discovery of social media to reduce volume and address legitimate privacy interests of parties and non-parties. For example, access to "private" social media content may be conditioned on a showing of relevance based on public postings. Alternatively, an attorney may be directed to search his client's private postings to determine and produce what is responsive to

discovery requests. A judge could also conduct an *in camera* review or appoint a court-appointed neutral to do so. That, in turn, might lead to the issuance of a Rule 26(c) protective order to protect privacy interests.

6.3.6 Require the parties to consider privacy interests of parties and non-parties and, if appropriate, consider issuance of a Rule 26(c) protective order limiting access to the ESI.

6.3.7 When transnational discovery is in dispute, require the parties to address any foreign law governing the production of *protected* ESI and consider, as an alternate to production, ordering the requesting party to proceed by first seeking data located domestically or by letters rogatory.

6.3.8 Consider *sequencing* or *phasing* eDiscovery, focusing on discovery of ESI directly related to claims and defenses in the pleadings in the first instance to expedite the discovery process and, if in state court, deferring rulings on broader eDiscovery requests until the first phase is completed.

6.4 Representative decisions

6.4.1 *Hardy v. UPS Ground Freight, Inc.*, Civil Action No. 3:17-cv-30162-MGM, 2019 WL 3290346, at *2 (D. Mass. July 22, 2019) (denying defendant's motion to compel forensic examination of plaintiff's cell phone because defendant failed to

"articulate a basis for an accusation that Plaintiff may have engaged in spoliation of evidence.").

6.4.2 *Rodriguez-Ruiz v. Microsoft Operations Puerto Rico, L.L.C.*, Case 3:18-cv-01806-PG, 2020 WL 1675708 (D.P.R. Mar. 5, 2020) (ordering production of plaintiff's social media content reflective of emotional state; content to be reviewed and produced by his counsel rather than by allowing defendant to have unrestricted access to plaintiff's account).

6.4.3 *Adamson v. Pierce Cnty*, Case No. 3:21-cv-05592-TMC, 2023 U.S. Dist. LEXIS 197983 (W.D. Wash. Nov. 3, 2023) (allowing discovery on alleged destruction of text messages and text message policies of defendant due to its inadequate explanation of gap in production).

6.4.4 *United States ex rel. Gill v. CVS Health Corp.*, No. 18 C 6494 (N.D. Ill. Feb. 15, 2024) (court admonishing parties for "excessive vexatiousness" and warning that it would consider drastic measures to address such conduct).

6.4.5 *Forman v. Henkin*, 30 N.Y.3d 656 (2018) (threshold inquiry as to whether social media postings are discoverable was not whether the materials sought were private but whether they were reasonably calculated to contain relevant information).

6.5 Further reading

6.5.1 The Sedona Conference, *Commentary on Rule 34 and 45 "Possession, Custody, or Control,"* 17 SEDONA CONF. J. 467.

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

6.5.3 The Sedona Conference, *Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1 (2019.

6.5.4 Hon. Craig B. Shaffer, *Deconstructing "Discovery About Discovery,"* 19 SEDONA CONF. J. 215 (2018.

6.5.5 The Sedona Conference, *The Sedona Conference Commentary on Ephemeral Messaging*, 22 SEDONA CONF. J. 435 (2021.

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

7. Proportionality

7.1 Proportionality as a concept

7.1.1 Discovery can be expensive. Indeed, some argue that discovery costs and burdens, particularly those related to ESI, are so expensive that those costs prevent parties from fairly and fully litigating claims and defenses in federal or state courts. Judges should be mindful of such arguments when addressing costs and burdens.

7.1.2 One obstacle to proportionality may be broad discovery requests and objections that lead to disputes about relevance, scope, and disproportionality. The 2015 amendments to the Federal Rules were intended to require specificity in both requests and objections. State rules might not impose such a specificity requirement.

7.1.3 Rule 26(b)(1) makes clear that *all* discovery is subject to proportionality. The rule describes a cost-benefit analysis that a judge must perform in permitting parties to engage in what might be costly and time-consuming eDiscovery. Although states may or may not have adopted similar rules, state judges often engage in proportionality analyses—however these may be expressed—in ruling on discovery requests. Although judges might prefer that the parties engage in a proportionality analysis—and Rules 1, 26(b)(1), and 26(g)(1)(B)(iii) require this analysis to be undertaken by attorneys—the exercise of proportionality by federal and state judges is perhaps the strongest tool available to manage discovery.

7.1.4 Proportionality is inherently an amorphous concept. Rule 26(b)(1) lists six factors—set forth in Section IV.6.1.3 above—that a judge should take into consideration, but, as the comments to the 2015 amendment to that rule make clear, the list is nonexclusive. Moreover, the factors are not listed in any order of priority, and although cost may be a factor, it may not be determinative.

7.2 Issues presented

7.2.1 There may be objections raised to one or more discovery requests based on allegations that they are disproportionate to the needs of a particular case. Such objections present a judge with the question of whether to direct the parties to confer in an attempt to reach resolution and report back.

7.2.2 Should the parties not be able resolve their dispute, the judge will need to consider how to allocate the burden of proof on the proportionality objection, whether to conduct a hearing with witnesses, or whether to proceed only with written submissions.

7.2.3 The resolution of proportionality disputes may impact a judge's overall management of a particular case. He should consider how the resolution of the disputes may impact existing scheduling orders.

7.3 Suggested judicial management strategies

7.3.1 Direct the parties to confer in an attempt to resolve any proportionality dispute and have the parties report back on the success or failure of that conference. Incorporate any agreements into a case management order. Consider requiring the parties to file a joint letter to the court outlining any disagreements in lieu of formal motion practice.

7.3.2 Advise the parties whether formal motion practice will be required to bring the dispute before the court or whether the dispute can be presented by affidavit or written proof.

7.3.3 Allocate burden of proof before any argument or submission. Given the nature of proportionality, the requesting party should not be expected to demonstrate cost or burden on the objecting party. It should, however, be expected to demonstrate relevance and specificity. The objecting party should then bear the burden to demonstrate, with an appropriate factual showing, that the discovery sought would be disproportionate to the needs of the case because of excessive cost for retrieval or privilege review, privacy concerns, business interruption, the availability of the information from less expensive alternative sources, delay in the case, etc.

7.4 Representative decisions

7.4.1 *In re Mercedes-Benz Emissions Litig.*, No. 16-cv-881, 2020 WL 487288 (D.N.J. Jan. 30, 2020) (defendant ordered to produce information related to its German employees; proportionality objection based on GDPR rejected but protective order issued to obviate objection).

7.4.2 *Pentel v. Shepard*, No. 18-cv-1447, 2019 WL 3729770 (D. Minn. Aug. 7, 2019) (production of three years' worth of database inquiries requiring 102, 200 separate searches and review of 306,600 pages found disproportionate).

7.5 Further Reading

7.5.1 The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141 (2017.

7.5.2 Hon. Craig B. Shaffer, *The "Burdens" of Applying Proportionality*, 16 SEDONA. CONF. J. 55 (2015).

7.5.3 R.D. Keeling & R. Mangum, *The Burden of Privacy in Discovery*, 20 SEDONA CONF. J. 414, 441 (2019).

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

8. Identification of "not reasonably accessible" sources of ESI

8.1 Rule 26(b)(2)(B)

8.1.1 Rule 26(b)(2)(B) provides that a party need not produce ESI from sources that a party identifies as being not reasonably accessible because of undue burden or cost. If a requesting party persists in requesting ESI from those sources, the judge must determine whether the sources are, in fact, not reasonably accessible. If the requested information is not reasonably accessible but *good cause* exists to produce ESI from those sources, the judge may order the ESI to be produced under the proportionality limitations of Rule 26(b)(2)(C) and also may impose other conditions, including cost sharing or cost shifting.

8.1.2 *Production* of ESI from sources that are not reasonably accessible is distinct from *preservation* of

that ESI. Identification of a source of ESI as being not reasonably accessible does not relieve the party of the obligation to preserve evidence, absent agreement of the parties or order of the court.

8.2 Issues presented

8.2.1 Identification or description of the alleged "not-reasonably-accessible" source is necessary. The Advisory Committee Notes to the 2006 amendment to Rule 26(f) suggest that parties discuss whether ESI is reasonably accessible. This discussion should be in sufficient detail so that the requesting party can make an informed determination whether to seek production from any source not being searched.

8.2.2 The burden is on the party making the assertion that a source is not reasonably accessible to prove the source is, *in fact*, not reasonably accessible.

8.2.3 If the responding party shows that the source is not reasonably accessible, but the requesting party presses its request for production, the court must determine whether *good cause* exists for the production. The Advisory Committee Notes to the 2006 amendment of Rule 26(b)(2)(B) suggest that a court may consider a number of factors in determining whether good cause exists. One factor may be whether the source was rendered not reasonably accessible by the action or inaction of the responding party.

8.2.4 As technology advances, what is and is not considered "reasonably accessible" will change. For instance, "backup tapes" were considered a *per se* "not reasonably accessible" source of ESI when the seminal *Zubulake*[12] case was decided. Twenty years later, access to ESI from backup media is not considered particularly burdensome or costly.[13]

8.3 Suggested judicial management strategies

8.3.1 Direct the party asserting that ESI is not reasonably accessible to identify any accessible sources where the ESI can be found or third parties that may have it on an accessible source.

8.3.2 Phase or limit discovery in the first instance to ESI from accessible sources and defer any consideration of discovery from sources that are not reasonably accessible until after an assessment of further need can be made.

8.3.3 Allow the parties to engage in *focused* and *limited* discovery to test whether, in fact, the ESI source is or is not "reasonably accessible."

---

12. Zubulake v. UBS Warburg ("Zubulake I"), 217 F.R.D. 309 (S.D.N.Y. 2003)

13. For a useful list of factors to consider in determining the accessibility of a source of ESI, see The Sedona Conference, *Commentary on Preservation*, The Sedona Conference, *Management and Identification of Sources of Information that are Not Reasonably Accessible*, 10 SEDONA CONF. J. 281, 290 (2009).

8.3.4 Direct the requesting party to narrow its requests to minimize any undue burden or cost, or shift costs in whole or in part.

8.3.5 Require the parties to present expert testimony, if necessary, on whether the source of the requested ESI is not reasonably accessible. Alternatively, require the parties to proffer testimony by information technology personnel.

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

9. Search and collection methodologies

9.1 One goal of judicial case management should be to encourage parties to agree on a search and collection methodology *before* discovery begins. Such an agreement should reduce cost and delay and conserve judicial resources. Defining such a methodology in terms of date ranges, data sources, file type, and likely custodians enables parties to conduct eDiscovery in an efficient and cost-effective way. While traditional methods of identification and collection (interviews with custodians, manual searches through files, etc.) have their place, cost savings might be realized if parties agree to use automated search and collection technologies, particularly with larger collections. The more transparency and cooperation between the parties in the application of these technologies, the less the likelihood that parties will dispute the results.

9.2 Issues presented

9.2.1 Parties are not accustomed to sharing, let alone negotiating, the methodology they intend to use for search and collection of ESI. This resistance is compounded by concern that selection criteria may reveal the mental processes of counsel and constitute work product.

9.2.2 Parties *requesting* ESI are often unaware of the search and collection methodologies that might be available to the *responding* party. For example, the requesting party is unlikely to know how the responding party has organized its ESI or what search criteria could yield the most relevant and useful information.

9.2.3 Parties may not be familiar with advanced technological tools to reduce the cost of manual search and collection procedures. These tools may bear names such as, among others, Technology-Assisted Review (TAR), predictive coding, or machine learning. These technologies are intended to limit the need for manual review of large volumes of ESI for relevance and privilege. Properly used, such technologies may substantially decrease the cost and delay normally associated with document review.[14] However,

14. In 2012, the ABA added Comment 1.8 to Model Rule of Professional Conduct 1.1 on Competence to emphasize that "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." At least 38 states have followed with amendments to their own Professional Conduct codes and the institution of

existing case law is sparse and, in the final analysis, merely finds that a particular technology is *reasonable*. Few courts have reviewed the *results* of an automated search and found that those results were reasonable. Moreover, there is no accepted definition of the *reasonableness* of an automated search.

9.2.4 Automated search raises another unanswered question: It may be necessary for a qualified expert to opine on the reliability of advanced search and collection technologies under Federal Rule of Evidence 702 or its state equivalent. Alternatively, a more lenient standard of *reasonableness* might be the measure.

9.2.5 Finally, parties may fear that a court will reject a specific technological tool or method as being *unreasonable*, resulting in the need to repeat a search or production, the loss of privilege or work-product protection, or a sanction. This fear may be reduced or eliminated if the parties reach agreement on a tool or method and present that agreement to a court as a stipulation binding the parties. Absent such agreement, the party proposing to use a specific method may seek prior judicial approval.

9.3 Suggested judicial management strategies

---

technology-focused continuing legal education requirements. For a complete list and links to the individual rules, see LawSites, Tech Competence, at https://www.lawsitesblog.com/tech-competence.

9.3.1 Encourage the parties to agree in advance on an appropriate methodology, depending on the needs of the case and nature of the information to be collected. Judges should be familiar with the options available, but parties are in the best position to determine the best methodology for locating and collecting responsive ESI.[15]

9.3.2 Encourage the parties to collaborate on a sample search of ESI to determine the most effective search methodology to apply to a larger collection.

9.3.3 If keyword searching is considered by the parties to be an appropriate methodology, encourage the parties to agree to reasonable set of keywords. Avoid having the court be forced to select keywords for the parties, as the court is not able to determine whether any given set of key words will be effective in retrieving relevant information and filtering out irrelevant information.

9.3.4 Direct the parties to attempt to reach agreement on the use of automated search technologies if appropriate given the needs of a particular case and advise that insistence on the use of costly

15. *See* The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production,* 19 SEDONA CONF. J. 1 *(2018).* ("Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.") and associated Comments.

and time-consuming manual procedures will be viewed with skepticism.[16]

9.3.5 Consider staging searches, focusing on those active data sources most likely to yield relevant information. *Staging* here means staging by data source rather than issue, as is often employed in complex litigation.

9.4 Representative decisions

9.4.1 *City of Rockford v. Mallinckrodt ARD Inc.*, No. 17 CV 50107, 326 F.R.D. 489, 495 (N.D. Ill. 2018) (adopting agreed-on order establishing production protocol for ESI with "inclusion of Plaintiffs' proposal that a random sample of the null set will occur after the production and that any responsive documents found . . . will be produced.").

9.4.2 *Nuvasive, Inc. v. Alphatec Holdings, Inc.*, 557 F. Supp. 3d 1069 (S.D. Cal. 2021) (citing Sedona Principle 6; denying motion to compel party to search its ESI using search terms proposed by moving party)

9.4.3 *Humanmade v. SFMade*, Case No. 23-cv-02349-HSG (PHK) (N.D. Ca. July 10, 2024) (establishing

16. *In re Mercedes Benz Emissions Litig.*, No. 16-cv-00881, 2020 WL 103975 (D.N.J. Jan. 9, 2020) (discovery master declines to order defendant to utilize TAR to identify responsive documents but cautions that future objections based on the cost of review will not be looked kindly upon).

procedure for parties to adhere to regarding dispute over seven search terms)

9.5 Further reading

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

9.5.2 The Sedona Conference, *The Sedona Conference, Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* 25 SEDONA CONF. J. 1 (2024).

9.5.3 The Sedona Conference, *The Sedona Conference, Primer on Crafting eDiscovery Requests with "Reasonable Particularity,"* 23 SEDONA CONF. J. 337 (2022).

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

10. Form or forms of production

10.1 ESI exists, and can be produced, in various forms. Form of production can be a particularly contentious issue in eDiscovery. Parties can dispute whether ESI should be produced in, for example, paper, portable document format (PDF), tagged image file format (TIFF), or native form. This section addresses form of production and why a particular form or forms may be appropriate for the needs of a particular action.

10.2 Issues presented

10.2.1 Parties may neglect to follow the process by which a particular form or forms may be requested. Rule 34(b) permits a party to specify the form or forms in which it wants ESI produced. This is intended to "facilitate the orderly, efficient, and cost-effective discovery of electronically stored information."[17] Absent such a specification, "the responding party must produce electronically stored information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable."[18] If the requesting party is not satisfied with the form stated by the responding party, or if the responding party has objected to the form specified by the requesting party, the parties must confer under Rule 37(a)(2)(B) in an effort to resolve the dispute.

10.2.2 If a court is forced to resolve the dispute, "the court is not limited to the forms initially chosen by the requesting party, stated by the responding party, or specified in [the] rule . . . ."[19]

10.2.3 Rule34(b)(2)(E)(i) directs that a "party must produce documents as they are kept in the *usual course of business* or must organize and label them to correspond with the categories in the

17. FED. R. CIV. P. 34(b) advisory committee's note to 2006 amendment.

18. *Id*.

19. *Id*.

request . . . ." (Emphasis added.) However, Rule 34(a)(1)(A) also permits the discovery of "any documents or electronically stored information . . . after translation by the responding party into a *reasonably usable form* . . . ." (Emphasis added.) Thus, the default form of production should be the form in which the ESI is kept in the "usual course of business" or, alternatively, in a "reasonably usable form."

10.2.4 A responding party may produce ESI in a form that is not in a "reasonably useable form" as required by the rule. This may be because the ESI has been produced in an unusual or proprietary format requiring specialized software to be searched or read, or in a jumbled and disorganized fashion, or in such large volume as to frustrate any effective review. This may also be the result of the parties' failure to confer on the appropriate format prior to production, a failure of the requesting party to understand the consequences of its request, or an intentional effort by the responding party to "hide the ball."

10.2.5 A second and more contentious issue arises from requests that seek a form that incorporates "metadata." Metadata refers to ESI that is not apparent from the face of a given electronic "document" and may disclose, for example: the dates of creation, edits, and comments; file size and location; deletion dates and times; access and distribution; authorship or the username associated with those tasks.

10.2.6 Metadata also provides a means by which a party can conduct a meaningful and relatively inexpensive search of an adversary's ESI. While the metadata itself may not be relevant to any claim or defense in a particular action, some types of metadata serve a useful purpose in helping the parties access and review relevant ESI.

10.2.6.1 Metadata may show the history of a backdated document or a party's improper attempts to delete relevant ESI. Thus, there are circumstances where metadata may be highly relevant.

10.2.6.2 The number of fields of metadata associated with particular sources of ESI is always expanding, as computer applications become more complex and require more sophisticated behind-the-scenes management. For instance, the "Dublin Core" set of metadata terms used in the first automated card catalogue system consisted of 15 fields (title, author, publication date, etc.) to describe every book in a library. Today, an email message or word-processed document could have hundreds of metadata fields associated with it, of which only a handful would likely be relevant or useful in litigation.

10.3 Suggested judicial management strategies

10.3.1 Direct the parties to describe the manner in which they collect and preserve ESI at their initial Rule 26(f) conference so that the parties can discuss the appropriate form or forms of production. Emphasize to the parties that an informal discussion may minimize or eliminate cost and undue delay.

10.3.2 In an action pending in state court that does not have an equivalent to Rule 34(b), direct the parties to look to Rule 34(b) for guidance.

10.3.3 Apply Sedona Principle 12, which provides that, in the absence of agreement or an order, production "should be made in the form or forms in which it is ordinarily maintained or that is reasonably usable given the nature of the electronically stored information and the proportional needs of the case."[20]

10.3.4 Require the requesting party to demonstrate why production of ESI should be in a particular form or forms and require a producing party to demonstrate why production of ESI in a particular form or forms does not unreasonably diminish its usability. For example, assume that a producing party proposed to produce a PDF of a spreadsheet. The PDF would not be useable in

20. The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 169 (2018).

that form if the requesting party sought to learn how each cell in the spreadsheet had been populated. To be useable the spreadsheet would need to be produced in native form, showing the formulae or source of each cell's data. Conversely, assume that a producing party proposed to produce an email as a PDF. If the requesting party sought the email for its content as the email had been transmitted then, presumably, the pdf would be useable. If, however, the requesting party intended to argue that the content had been modified after transmission then native might be required.

10.4 Representative decisions

10.4.1 *Frey v. Minter*, No. 4:18-CV-191, 2019 WL 5268548 (M.D. Ga. Oct. 17, 2019) (production of ESI in single 156-page PDF found "reasonably useable").

10.4.2 *Ice Cube Bdngs. LLC v. Scottsdale Ins. Co.*, No. 17-cv-00973, 2019 WL 4643609 (D. Conn. Apr. 8, 2019) (defendant's production of ESI found "reasonably useable," but defendant ordered to produce "Table of Contents or similarly structured document").

10.4.3 *In re: Uber Tech., Inc., Passenger Sexual Assault Litig.*, No. 23-md-3084, 2024 WL 1772832 (N.D. Ca. Apr. 23, 2024) (declining to order that parties' ESI protocol include obligation to produce contemporaneous versions of documents hyperlinked in e-mail or chats).

10.4.4 *In re StubHub Refund Litig.*, No. 20-md-02951-HSG (TSH), 2024 WL 2305604 (N.D. Ca. May 20, 2024) (granting motion to modify parties' ESI protocol to remove obligation to produce hyperlinked documents).

10.5 Further reading

10.5.1 The Sedona Conference, *Federal Rules of Civil Procedure 34(b)(2) Primer: Practice Pointers for Responding to Discovery Requests*, 19 SEDONA CONF. J. 447 (2018.

10.5.2 D. Greetham, *E-Discovery Hyperlinks Debate Won't Resolve Technical Challenges*, BLOOMBERG LAW (June 27, 2024).

10.5.3 *Hyperlinks to Documents Are Not the Same as Traditional Attachments*, FREDRIKSON LEGAL UPDATES (June 27, 2024).

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

11. Confidentiality and public access

11.1 This is a topic that may be raised in any civil action, state or federal. Rule 26(c)(1) (and its state equivalents) allows a party to "move for a protective order in the court where the action is pending." The court may, for good cause, issue an order "to protect a party from annoyance, embarrassment, oppression, or undue burden

or expense" for a number of reasons, including the confidential nature of a document.[21]

11.2 Issues presented

11.2.1 Parties will often proposed discovery protective orders with numerous categories of permitted or prohibited access, such as categories designated as "attorneys' eyes only," intended to prohibit access by particular parties, witnesses, or consultants. Unless these categories are justified and clearly delineated, they can result in confusion, delay, and ancillary disputes. The court should encourage simplicity.

11.2.2 There is a fundamental distinction between the burden imposed on a party to secure a confidentiality order and the burden imposed on a party to secure a filing under seal. The latter implicates First Amendment and common-law-based rights of access. This fundamental distinction requires a judge to: (a) appreciate the distinction and (b) apply the compelling interest test when *filing under seal* is sought.

11.2.3 Beyond protecting privilege and work product, parties often seek to protect information that might, for example, constitute a trade secret or reveal highly personal matters. If exchanged without some type of restriction of use or dissemination, that information may become known to the public at large. Parties seeking

21. FED. R. CIV. P. 26(c)(1)(A-H).

protection for these types of information must look to Rule 26(c) or its state equivalents.

11.2.4 Parties are often under the impression that social media postings, when designated as "private," are shielded from discovery or can only be produced under a protective order. The privacy settings offered by social media platforms do not confer any special legal status, and these postings are discoverable if relevant, non-privileged, and proportional to the needs of the case. See Section 6.2.2 above.

11.3 Representative decisions and orders

11.3.1 *Kannan v. Apple Inc.*, Case No. 17-cv-07305-EJD (VKD), 2019 WL 3037591 (N.D. Cal. July 11, 2019) (permitting defendant to produce confidential records of defendant's employees on attorneys'-eyes-only basis to plaintiff's counsel and directing that counsel not share contents with plaintiff).

11.3.2 Western District of Texas Local Civil Rules, Appendix H ("Confidentiality and Protective Order").

11.4 Further reading

11.4.1 The Sedona Conference, *The Sedona Guidelines: Best Practices Addressing Protective Orders, Confidentiality & Public Access in Civil Cases*, 8 SEDONA CONF. J. 141 (2007).

11.4.2 The Sedona Conference, *The Sedona Conference Commentary on the Need for Guidance and Uniformity in Filing ESI and Records Under Seal*, 23 SEDONA CONF. J. 379 (2022).

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

12. Protection of attorney-client privilege and work product

12.1 Protection of attorney-client privilege and work product goes to the heart of the adversary system. Production of ESI can often be voluminous and contain privileged information, stored in nonapparent locations such as metadata. This leads to the risk that such information may be inadvertently produced or produced without adequate protection.

12.2 Issues presented

12.2.1 Responding parties that withhold relevant documents on privilege or work-product grounds are almost universally required to provide a privilege log identifying the withheld documents and stating why the documents were withheld.[22]

12.2.2 Rule 26(b)(5)(B) establishes a default procedure for asserting claims of privilege after production of information in discovery. If privilege or work product is asserted over produced information, the producing party must timely notify the

22. *See, e.g.*, FED. R. CIV. P. 26(b)(5)(A).

receiving party, who is obligated to "promptly return, sequester, or destroy the specified information and any copies it has." The information should then be identified on a privilege log, subject to judicial resolution if challenged. "The producing party must preserve the information until the claim is resolved."

12.2.3 Rule 26(b)(5)(B) is a procedural rule and does not afford any substantive protection for attorney-client communications or work-product material produced during discovery. While the *procedure* is designed to reduce cost and delay associated with disputes over inadvertently produced privileged documents and ESI during discovery, production itself may give rise to a waiver in many state courts. Prior to 2008, this was also true in many federal courts, and the scope of waiver may have extended to all information regarding the same subject matter as the inadvertently produced information.

12.2.4 Therefore, the risks associated with inadvertent production of privileged information have been very high; consequently, the cost of privilege review is often cited as a major component of the overall cost of litigation.

12.2.5 Federal Rule of Evidence 502 was enacted in 2008 to address these concerns. A number of states have adopted equivalents to Rule 502, but note that some have adopted only particular sections of that rule.

12.2.6 Rule 502(a) limits the risk of subject-matter waiver to instances in which the waiver was intentional.

12.2.6.1 Rule 502(b) establishes *somewhat* uniform standards throughout the federal courts to resolve claims of waiver by inadvertent production, adopting a three-part test to determine if an inadvertent production constitutes a waiver.

12.2.6.2 Rule 502(e) allows parties to enter into nonwaiver agreements that are binding only as to those parties.

12.2.6.3 Rule 502(d) has the greatest potential for cost savings and efficiencies. It provides for nonwaiver confidentiality orders under which parties can disclose ESI and other information in discovery without waiving attorney-client privilege or work-product protection. Such an order is binding in any other federal and state proceeding.

12.3 Suggested judicial management strategies

12.3.1 Direct that the parties confer on privilege and confidentiality issues before discovery begins and before presenting any disputes to the court.

12.3.2 Direct the parties to attempt to agree on issues of waiver and protection of confidential information, and that any resulting agreements be

presented to the court at the initial case management conference and incorporated in the court's Rule 16 scheduling order.

12.3.3 Consider entering a nonwaiver confidentiality order with or without the parties' agreement under Federal Rule of Evidence 502(d) or its state equivalent, after providing the parties with an opportunity to express any concerns about such an order. In entering such an order, be aware of the confusion that sometimes exists between orders under sections (b) and (d) of this rule and remind the parties of the distinction between such orders so that they appreciate what they are agreeing to.

12.3.4 If the parties cannot agree on a nonwaiver order, the federal rule allows the court to enter an order under Rule 502(d) *sua sponte*, and state courts may also have that power if they have an equivalent to Rule 502.

12.3.5 Establish a procedure by which challenges to privilege or confidentiality assertions can be addressed in the most timely and efficient manner, ideally before disputed documents appear in depositions or as attachments to motions. Federal Rule of Civil Procedure 26(b)(5)(B) provides a default procedure.

12.3.6 In the event that the privilege or confidentiality designations of a large volume of documents are challenged, direct the parties to attempt agreement on *categorizing* disputed information so

that a ruling on samples will apply to each category.

12.4. Representative decisions, orders, and local rules

12.4.1. *Ingham Reg'l Med. Ctr. v. United States*, 146 Fed. Cl. 424 2020) (work-product protection not available for information prepared in general course of business rather than in anticipation of business).

12.4.2. *Proxicom Wireless, LLC v. Target Corp*., No. 6:19-cv-1886, 2020 WL 1671326 (M.D. Fla. Mar. 25, 2020) (Rule 502(d) held not to protect "proprietary and confidential" materials; applicable to attorney-client communications and work product).

12.4.3 District of New Jersey, Local Civil Rule 16.1, provides: Absent objection of a party or a form of order submitted on consent, either of which must be set forth in a proposed discovery plan submitted pursuant to Federal Rule of Civil Procedure 26(f)(2), a scheduling order entered pursuant to this subsection on or after September 30, 2016 shall be deemed to incorporate an order pursuant to Federal Rule of Evidence 502(d) that:

(i) The production of materials, inadvertent or otherwise, shall not be deemed a waiver of attorney-client privilege or work product protection in this civil action or in any other federal or State proceeding.

(ii) Nothing in (i) above shall limit the right of a party or subpoenaed nonparty to conduct a reasonable review of materials for relevance or otherwise in response to a discovery request or requests.

12.4.4 *Linet Am. Inc. v. Hill-Rom Holdings, Inc.*, Case No. 1:21-cv-6890, 2024 U.S. Dist. LEXIS 123910 (N.D. Ill. July 15, 2024) (holding, among other things, that federal common law applies to "at issue" waiver analysis, that implied waiver requires reliance on privileged communications, and that allegations of spoliation does not warrant finding of implied waiver).

12.4.5 Southern District of New York, Rule 502(d) Order.

12.5 Further reading

12.5.1 The Sedona Conference, *Commentary on the Protection of Privileged ESI*, 17 SEDONA CONF. J. 95 (2015).

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

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

13. The privilege log

13.1 Rule 26 (b)(5)(A) prescribes the preparation of a timely privilege log and, in general, describes its contents. The form or content of privilege logs may also be supplemented by local rules or chambers practices.

13.1.1 Absent agreement between the parties to forego these, privilege logs are essential to judicial resolution of disputes between parties about withheld information. Nevertheless, especially with ESI, privilege logs can be voluminous, a major source of satellite litigation, and a substantial drain on both party and judicial resources.

13.2 Issues presented

13.2.1 The parties must be clear on the level of detail that a privilege log should contain. Rule 26(b)(5)(A)(2) requires that a party "describe the nature of the documents . . . and do so in a manner that . . . will enable other parties to assess the claim." This does not offer concrete guidance about what form a log should take. Absent party agreement, the court must prescribe the form. For example, logged email might include such metadata fields as "to," "from," "cc," "bcc" or the like. Should other metadata fields be included? Judges should be wary of automatically generated privilege "logs" based on arbitrary criteria, such as the simple phrase "attorney-client privilege" or the name of an attorney appearing in a document.

13.2.2 Privilege logs should be sufficiently specific to allow a reviewing party to accept or challenge a claim of privilege. For example, it might be insufficient to describe a document as "giving legal advice."

13.2.3 As noted above, privilege logs can be voluminous. As an alternative to requiring every document on a log to be described, parties might be directed to fully describe exemplars of documents in each of several categories. Indeed, Local Rule 26.2(c) of the Southern and Eastern Districts of New York consider such categorical privilege logs to be "presumptively proper."

13.2.4 Message strings (or "threads") consist of related email communications over time, initiated by a "parent" message. The parent message may be an attorney-client communication or work product, the status of which may not be obvious later in the string. Judges should consider alternatives to describing each message on a string. For example, a judge might direct a party to describe only privileged messages on a string. Alternatively, it might be sufficient to log only the "latest" message on a string that includes a privileged message. Moreover, it might be unnecessary to log nonprivileged communications in a string?

13.3 Suggested judicial management strategies

13.3.1 At the initial conference between the parties, encourage them to agree on the definition of

privileged communications and work product as a precursor to any discussion of privilege logs. This and related agreements on topics such as those described below should be incorporated into stipulations under Rule 29 or its state equivalents.

13.3.2 Require the parties to address the form and content of privilege logs at the initial conference between the parties.

13.3.3 Require the parties to attempt to agree on a reasonable time to produce a privilege log, which may be more than the time otherwise allowed by local rule or practice if voluminous ESI must be logged.

13.3.4 Encourage the parties to identify presumptively privileged documents that may be segregated and excluded from production based on some agreed methodology; for example, communications with outside counsel after the filing of a complaint or answer.

13.3.5 Encourage the parties to agree that otherwise voluminous logs be prepared more economically; for example, by category of items rather than individual listing of each document.

13.3.6 Encourage the parties to agree on how message strings should be logged.

13.3.7 Require the designating party to submit an affidavit or affidavits that, for example, identify all

persons named on a log and describe in greater detail why a particular document or documents are privileged.

13.3.8 If necessary, conduct an *in camera* review or refer disputes about logs to a court-appointed neutral. If the volume of disputed designations is onerous, consider reviewing a representative or random sample of the documents and entries.

13.4 Representative local rule

13.4.1 Joint Southern and Eastern Districts of New York, Local Civil Rule 26.2(c), provides:

Efficient means of providing information regarding claims of privilege are encouraged, and parties are encouraged to agree upon measures that further this end. For example, when asserting privilege on the same basis with respect to multiple documents, it is presumptively proper to provide the information required by this rule by group or category. A party receiving a privilege log that groups documents or otherwise departs from a document-by-document or communication-by-communication listing may not object solely on that basis, but may object if the substantive information required by this rule has not been provided in a comprehensible form.

COMMITTEE NOTE

With the advent of electronic discovery and the proliferation of e-mails and e-mail chains, traditional document-by-document privilege logs may be extremely expensive to prepare, and not really informative to opposing counsel and the Court. There is a growing literature in decisions, law reviews, and other publications about the need to handle privilege claims in new and

more efficient ways. The Committee wishes to encourage parties to cooperate with each other in developing efficient ways to communicate the information required by Local Civil Rule 26.2 without the need for a traditional privilege log. Because the appropriate approach may differ depending on the size of the case, the volume of privileged documents, the use of electronic search techniques, and other factors, the purpose of Local Civil Rule 26.2(c) is to encourage the parties to explore methods appropriate to each case. The guiding principles should be cooperation and the 'just, speedy, and inexpensive determination of every action and proceeding.' Fed. R. Civ. P. 1. See also *The Sedona Cooperation Proclamation*, whose principles the Committee endorses.

13.5 Representative decisions

13.5.1 *Coker v. Goldberg & Assocs. P.C.*, No. 21-cv-1803, 2024 WL 263121 (S.D.N.Y. Jan. 24, 2024) (finding, among other things, that defendant waived privilege claims for failure to file timely privilege log).

13.6 Further reading

13.6.1 *The Sedona Conference Commentary on Privilege Logs* (May 2024).

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

14. Allocation of costs during litigation

14.1 The conduct of remote and hybrid proceedings may result in significant pretrial and trial cost reduction. The

refusal to engage in remote or hybrid proceedings, without good cause, may be a consideration in the allocation of costs.

14.2 Cost shifting came to eDiscovery with the iconic *Zubulake* decision[23] in the context of production of ESI from "inaccessible" sources. Cost shifting and cost sharing are implicit in Rule 26(b)(2)(B), under which "[t]he court may specify conditions for the discovery" of ESI from not-reasonably-accessible sources. Note that the court's discretionary power to allocate costs in the course of discovery are distinct from the post-judgement award of costs associated with discovery, which are more narrowly governed by rule and statute.

14.2.2 Cost shifting or cost sharing in discovery may appear to be inconsistent with the presumption, stated by the Supreme Court in *Oppenheimer Fund, Inc. v. Sanders*,[24] that each party bears its own litigation costs. The party seeking cost shifting or cost sharing bears the burden of overcoming that presumption by a preponderance of the evidence.

14.2.3 Rule 26(c)(1)(B) expressly authorizes federal judges to order "the allocation of expenses" related to discovery. The Advisory Committee notes to the 2015 amendment to this rule state that authority to allocate costs "is included . . . and courts already exercise this authority.

23. Zubulake v. UBS Warburg ("Zubulake I"), 217 F.R.D. 309 (S.D.N.Y. 2003)

24. 437 U.S. 340, 358 (1978)

Explicit recognition will forestall the temptation some parties may feel to contest this authority. Recognizing the authority does not imply that cost shifting should become a common practice. Courts and parties should continue to assume that a responding party ordinarily bears the costs of responding."

14.2.4 Rule 26(b)(2)(b) also expressly authorizes federal judges to allocate costs if not-reasonably accessible information is ordered to be produced, but it does so in oblique language: "The court may specify conditions for the discovery." The Advisory Committee notes to the 2006 amendment to the rule addresses costs expressly: "The conditions may also include payment by the requesting party of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible."

14.3 Issues presented

14.3.1 Cost-shifting or cost-sharing questions may not be limited to the production of ESI. However, production of ESI may result in significant costs, and parties may seek to have these costs shifted or shared. This should be discussed at the initial Rule 26(f) conference, if not sooner. There is little case law that addresses the allocation of costs. Sedona Proportionality Principle 1 suggests that the "burdens and costs of preserving relevant electronically stored information should be weighed against the potential value and

uniqueness of the information when determining the appropriate scope of preservation."[25]

14.3.2 There may be actions in which crucial ESI is known to be available only from sources that are not reasonably accessible under Rule 26(b)(2)(B). For example, email may no longer exist on accessible systems or word-processing documents from retired applications. In such instances, when a party has preexisting knowledge of such facts, the parties should be able to discuss cost shifting or cost sharing during the initial Rule 26(f) conference.

14.3.3 The Federal Rules do not set forth factors that guide the court's cost allocation analysis. What factors might be used? Factors suggested in the Advisory Committee notes to the 2006 amendments to Rule 26(b)(2)(B), concerning "good cause" for production of ESI from not-reasonably-accessible sources, may be informative. *Zubulake* set forth a related but slightly different set of factors specifically for cost shifting. Likewise, there is no uniformity among the state courts that have addressed this issue in the ESI context.

14.3.3.1 The *Zubulake* factors are:

(1) the extent to which the request is specifically tailored to discover relevant information

25. The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141, 146 (2017.

(2) the availability of such information from other sources

(3) the total cost of production compared to the amount in controversy

(4) the total cost of production compared to the resources available to each party

(5) the relative ability of each party to control costs and its incentive to do so

(6) the importance of the issue at stake in the litigation and

(7) the relative benefits to the parties of obtaining the information.[26]

14.4 Suggested judicial management strategies

14.4.1 Limit production of ESI to reasonably accessible information, the costs of which are presumably borne by the producing party.

14.4.2 Address cost shifting or cost sharing only after all relevant reasonably accessible information has been produced and reviewed by the requesting party.

14.4.3 Require the party seeking to allocate costs to describe in a detailed affidavit the cost and burden it expects to incur in producing ESI from sources it deems not reasonably accessible.

14.4.4 Require sampling of ESI that a party has been requested to produce from sources it deems not

26. Zubulake v. UBS Warburg, 217 F.R.D. 309, 322 (S.D.N.Y. 2003)

reasonably accessible, thus enabling the judge to ascertain the extent to which relevant information resides within the ESI and the cost of retrieval of the relevant data set.

14.4.5 Implement the above strategies when a producing party seeks to allocate costs for ESI due to undue burden or expense even if the ESI in issue is reasonably accessible through the application of the proportionality factors set forth in Rule 26(b)(1).

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

15. Discovery from non-parties

15.1 Discovery of ESI can be particularly troubling when non-parties are involved. Plainly, Rule 45 and its state equivalents allow such discovery. However, the ESI sought may be voluminous and expensive for a non-party to produce.

15.2 Issues presented

15.2.1 Promoting cooperation with respect to non-party subpoena practice can be both simpler and more difficult than discovery between the parties.

15.2.1.1 On the one hand, Rule 45 specifically provides that requesting parties and attorneys "must take reasonable steps to avoid imposing undue burden or

expense on a person subject to the subpoena." That rule also requires the court to protect non-parties from undue burden and expense, which may include an award of attorney's fees on parties or attorneys who fail to make reasonable efforts to avoid undue burden and expense.[27]

15.2.1.2 On the other hand, non-party involvement in discovery may complicate case management for a judge. For instance, Rule 45 has no requirement that the parties confer, so there is no formal mechanism for parties to work together to reduce costs and burdens. Moreover, subpoenaed non-parties may be outside the jurisdiction of the case-management judge. This may lead to more complication, as a court in another jurisdiction may be responsible for ruling on any dispute about the scope of a subpoena.

15.3 Suggested judicial management strategies

15.3.1 Encourage the parties in their initial Rule 26 conference to address any intent to secure information from non-parties and to include such intent in their discovery plan.

15.3.2 Direct the parties to present any dispute *between themselves* as to non-party discovery to the court

27. FED. R. CIV. P. 45(c)(1).

at the initial scheduling conference or as soon thereafter as possible.

15.3.3 Once a subpoena is served, request the issuing party and the subpoenaed non-party to confer in an attempt to resolve any of the latter's objections to the subpoena without formal motion practice.

15.3.4 Encourage the parties and the subpoenaed non-party to stipulate to an extension of time for the latter to object to the subpoena. The limited time period for objection under Rule 45(c)(2)(B) may frustrate any effort to resolve disputes amicably and without judicial involvement.

15.3.5 In the event that another judge has jurisdiction over the subpoena, *with the knowledge of the parties,* coordinate with that judge as to who will be responsible for ruling on any dispute. Under Federal Rule of Civil Procedure 45(f), when the court in which compliance of the subpoena is required is not the issuing court, the judge may transfer the subpoena dispute to the district that issued the subpoena if the person subject to the subpoena consents or the court finds exceptional circumstances.

15.4 Representative decisions

15.4.1 *In re Am. Kidney Fund, Inc.*, 2019 WL 1894248 (D. Md. Apr. 29, 2019) (cost shifting held not available under Rule 45(d) when non-party complied with subpoena voluntarily).

15.4.2 *Correct Transmission LLC v. Microsoft Corp.*, No. 2:23-MC-0075-KKE, 2023 WL 7301240 (W.D. Wash. Nov. 6, 2023) (court declined to order nonparty to produce documents sought by subpoena when documents could be obtained from another party)

15.5 Further reading

15.5.1 The Sedona Conference, *Commentary on Rule 45 to Non-Parties, Second Edition*, 22 SEDONA CONF. J. 1 (2021).

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

16. Discovery motion practice

16.1 Discovery motions can disrupt the timing of discovery and grow into satellite litigation where the merits of an action are pushed aside. Active judicial management of motion practice is essential and may eliminate or minimize motions.

16.1.1 Rule 26(c)(1) and Rule 37(a)(1) require a moving party to certify that it has, in "good faith," conferred or attempted to confer with the other affected parties in an attempt to resolve the dispute. The U.S. District Court for the District of New Jersey requires parties to bring any discovery dispute before a magistrate judge by conference call or letter prior to filing any formal

motion.[28] Going one step further, the U.S. District Court for the Eastern District of Texas maintains a *Discovery Hotline* so that parties can "get a hearing on the record and ruling on the discovery . . . "by a judge on discovery disputes.[29] These rules demonstrate an attempt to reduce formal motion practice in the federal courts, and many state courts have followed suit.

16.1.2 The Federal Rules also emphasize judicial involvement before a discovery motion is made. Rule 16(b)(3)(B)(iv) provides that a scheduling order may "direct that before moving for an order related to discovery, the movant must request a conference with the court."

16.1.3 Absent some prohibition under law, state judges who do not have the benefit of equivalents to Rule 16(b)(3)(B)(v) should also take steps to encourage informal resolution of discovery disputes.

16.2 Issues presented

16.2.1 Is the motion timely? Has the moving party exhausted reasonable alternatives to a formal motion? Has the responding party made, or offered to make, discovery that might obviate the need for a motion?

---

28. D.N.J., Loc. Civ. R. 37.1(a)(1).

29. E.D. Tex., Loc. R. CV-26(e).

16.2.2 Has the moving party made a sufficient showing to allow the motion to be decided? What proofs should the moving party make? The Federal Rules do not address burden of proof in general terms, however, the Advisory Committee notes to the 2015 amendment to Rule 37(e)(1) may be helpful:

16.2.3 Judges should be aware that expert reports submitted in support of, or in opposition to, discovery motions may be required to comply with Federal Rule of Evidence 702, its state counterpart, *Daubert*, or *Frye*. Such compliance may multiply the costs to the parties and the complexity of discovery motion practice.

16.3 Suggested judicial management strategies

16.3.1 Consider holding regular discovery conferences in complex civil actions to provide informal guidance to parties on emerging discovery disputes so as to avoid motion practice.

16.3.2 Advise the parties at the first case management conference that formal motion practice on discovery disputes is disfavored, and that the court expects parties to make good-faith efforts to resolve disputes on their own. Ensure that the parties confer pursuant to Rule 26(c)(1) or Rule 37(a)(1) or their state equivalents in an attempt to resolve any dispute.

16.3.3 Be available to resolve disputes informally and promptly should any arise or make

arrangements for a colleague to be available in a particular instance.

16.3.4 Require the parties to submit any dispute as a joint letter to the court requesting resolution.

16.3.5 Ensure that the parties confer pursuant to Rule 26(c)(1) or Rule 37(a)(1) or their state equivalents in an attempt to resolve any dispute.

16.3.6 Require that any formal motion to compel discovery include sufficient detail, including affidavits from competent persons if needed, which describe the nature of the dispute and the reason for the relief sought as well as, if appropriate, a detailed description of costs.

16.3.7 Require that the responding party describe why the discovery sought cannot or should not be allowed and, if appropriate, a detailed description of costs.

16.3.8 If warranted, address with the parties compliance with Federal Rule of Evidence 702, its state equivalents, *Daubert*, or *Frye*.

16.3.9 In the event that a hearing is necessary to resolve a discovery dispute, encourage the parties to agree to a video hearing to keep discovery moving and to help reduce the overall cost of litigation.

16.4 Representative decisions

16.4.1 Vallejo v. Amgen, Inc., 903 F.3d 733, 743 (8th Cir. Sept. 10, 2018) ("Rule 26 requires 'a particular and specific demonstration of fact, as distinguished from stereotyped and conclusory statement.'").

16.4.2 *Alcorn v. City of Chicago*, 336 F.R.D. 440 (N.D. Ill. 2020) (collecting cases addressing use of video recordings of remote depositions and suggesting procedures that parties might stipulate to).

16.4.3 *Flo. Bar v. James*, No. SC20-128, 2021 WL 5365639 (Fla. Nov. 18, 2021) (imposing 91-day suspension of attorney's license for texting his client with answers to questions during telephonic deposition).

16.4.4 *Stowe v. Alford*, No. 2:19-cv-01652 KJM AC, 2021 WL 2073750 (E.D. Cal. May 24, 2021) (setting forth protocol for remote deposition of plaintiff).

16.4.5 *Millelstadt v. Burgess*, [docket citation] 2025 WL 52555 (Ariz. Ct. App. Jan. 9, 2025) (affirming that, during deposition, party must answer any relevant, non-privileged question and that interlocutory appeal available under Arizona special action rule to challenge ruling below).

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

17. Evidential foundations

17.1 All civil actions should proceed as if these will be resolved by dispositive motion or trial. Discovery itself is intended to obtain ESI that will be admitted into evidence. These considerations may become lost on attorneys, parties, and judges.

17.2 Issues presented

17.2.1 Making a sufficient showing for admissibility of ESI may be difficult if the offering party has not kept sight of all the elements needed to establish foundation, relevance, and authenticity. Moreover, parties may need to retain experts to testify or submit affidavits in support of or in opposition to admissibility. Should a judge bring these matters to the attention of the parties early in the case management process or defer doing so until the dispositive motion or pretrial stage?

17.2.2 Parties may face particular problems should they seek to introduce into evidence ESI secured from non-parties, either voluntarily or through subpoena. Problems might arise from concerns about, among other things, form or forms of ESI that has been secured or business practices of the non-party that could lead to expensive deposition practice. To avoid this cost and burden and to minimize or eliminate disputes, parties should be encouraged to stipulate to the authenticity of ESI secured from non-parties.

17.2.3 Preliminary admissibility determinations are made by the court under Federal Rule of Evidence 104(a) or its state equivalents. The court is not bound by the rules of evidence in making these preliminary determinations and may be assisted by proffers from the offering party or its expert that are not subject to *Daubert* or *Frye* standards. Judges must consider when to make these determinations. They might do so at the pretrial stage of after commencement of trial. Judges should also consider whether there is a distinction in making the determinations for a nonjury as opposed to a jury trial.

17.2.4 Authentication of ESI may pose particular problems for trial management. First, ESI might not be self-authenticating under Federal Rule of Evidence 902. This concern may have been eliminated or at least minimized, however, by the adoption of Rules 902(13) and (14), effective December 1, 2017. The former addresses a "record generated by an electronic process or system that produces an accurate result." The latter deals with "[d]ata copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification." In either event, Rules 902(13) and (14) require the offering party to present a certification and give notice to other parties. A judge should presumably manage these requirements in such a way as to minimize delay.

17.2.5 Absent state equivalents to 902(13) and (14), how should a state judge address admissibility of ESI? Absent agreement between the parties, the judge may rely on "conventional" admissibility procedures, with special attention to the business record exception to the hearsay rule.

17.2.6 Federal Rule of Evidence 806(16) also addresses admissibility of ESI. It provides that, "[a] statement in a document that was prepared before January 1, 1998, and whose authenticity is established" is not excludable as hearsay "regardless of whether the declarant is available as a witness."

17.3 Suggested judicial management strategies

17.3.1 Remind the parties at the initial case management conference that, as they collect, produce, and review ESI, admissibility should be taken into account. This is especially important when ESI is produced by a non-party in response to a subpoena.

17.3.2 Remind the parties that depositions present opportunities to establish authentication for admissibility purposes, especially non-party depositions.

17.3.3 Direct the parties, before any dispositive motion or final pretrial conference, to stipulate to the admissibility of relevant ESI or to identify, by specific exhibit, what objections to admissibility are expected to be raised.

17.3.4 Direct the parties, absent stipulation, to serve Requests for Admission in order to establish authenticity.

17.4 Representative decisions

17.4.1 *State v. Knight*, A-37/38-23, 2024 N.J. Lexis (N.J. Dec. 18, 2024) (allowing jury to observe playback of surveillance video multiple times and in slow motion video surveillance but noting that "some tools or functions might be so specialized that their usage constitutes an alteration of evidence, or the creation of new evidence," and expert testimony may be required.)

17.5 Further reading

17.5.1 D.W. Linna Jr., , et al., *Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Materials in Nat'l Security Cases*, (August 08, 2024). NORTHWESTERN LAW & ECON RESEARCH PAPER NO. 24-18, NORTHWESTERN PUBLIC LAW RESEARCH PAPER NO. 24-26, available at https://ssrn.com/abstract=4943841 or http://dx.doi.org/10.2139/ssrn.4943841.

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

18. Presentation of electronic evidence at trials

18.1 ESI is commonly admitted into evidence at trial. Doing so, however, may present technical as well as scheduling problems for the parties and the trial judge. As with

evidential issues, the parties should plan and execute their eDiscovery with the use of ESI at trial in mind.

18.2 Issues presented

18.2.1 The form or forms of production that the parties agree to at the outset of discovery may influence the ability to use particular electronic presentation systems at trial.

18.2.2 Opposing counsel in a civil action may have different preferences as to the type of electronic evidence presentation system they want to use. The judge could encourage counsel to agree on a single system to be used at trial. Alternatively, assuming that the court has its own system available, the judge might need to address whether to allow counsel to use one that they prefer.

18.2.3 Opposing counsel may have different levels of skill in the preparation of electronic presentations or in the use of systems. All counsel must have adequate technical support.

18.2.4 The court should consider how to guard against the possibility that a jury will be confused or unduly influenced by the quality of the presentation and lose focus on the evidence being presented.

18.3 Suggested judicial management strategies

18.3.1 Suggest to the parties that they consider the method by which they intend to present

evidence at trial when negotiating the form or forms of production in discovery.

18.3.2 Require the parties to exchange information, not later than the final pretrial conference, about what evidence they intend to introduce in electronic form.

18.3.3 Require the parties to use any evidence presentation system available from the court. Moreover, require parties to become knowledgeable about the use of that system through, among other things, practice runs of their electronic evidence to avoid technical problems at trial. Consider having the courtroom available at a set time and day each week (e.g., Thursdays between 3 and 5 p.m.) for counsel who wish to conduct a practice run.

18.3.4 Assuming that there is no existing evidence presentation system, require the parties to agree on and use a common one and to become knowledgeable about its use. Make the courtroom available before trial to allow counsel to install and test their system.

18.3.5 Require the parties to have knowledgeable operators of the evidence presentation system present at trial.

18.3.6 Establish procedures for the jury's handling of the electronic evidence, including whether tablet computers that may be used by the jury in the courtroom can be taken into the jury room,

collecting and "scrubbing" such devices at the end of the trial, etc.

18.3.7 Direct the jury to maintain focus on the applicable significance of the electronic evidence, especially when such evidence is prone to distraction. be attentive to, but not mesmerized by, electronic evidence.

18.4 Sample orders

18.4.1. Procedures, Hon. Lee H. Rosenthal, U. S. District Court for the Southern District of Texas, Equipment (addressing technology available in the courtroom and the use of technology brought in by counsel).

18.4.2 U. S. District Court for the Eastern District of California, Electronic Evidence (requiring "[p]arties who intend to present evidence electronically via the Court's electronic evidence presentation systems [to] be familiar with the systems prior to the hearing/trial").

18.4.3 U. S. District Court for the Eastern District of California, Local Civil Rule 138(l), Submission of Audio and Video Files on Portable Media (addressing how evidence submitted electronically must be in a court-designated format).

18.4.4 U. S. Bankruptcy Court for the District of Maine, Electronic Evidence Presentation System (requiring "[p]arties who have never used the Court's system [to] schedule time in advance of

their reservation to practice and to test their electronic equipment's compatibility with the courtroom's system").

18.5 Representative decisions

18.5.1 *In the Interest of E.B.*, 507 P.3d 1092 (Colo. App. Jan. 6, 2022) (reversing termination of parental rights and remanding for new hearing when parent unable to participate remotely).

18.5.2 *In the Matter of Registrant J.P.A.*, Docket No. A-0452-20 (N.J. Super. Ct. App. Div. Jan. 12, 2022) (per curiam) (reversing sex offender classification and remanding for new hearing as respondent, not familiar with English, may not have understood how to appear virtually).

18.5.3 *Joffe v. King & Spalding LLP*, 17-CV-3392 (VEC) (S.D.N.Y. Dec. 10, 2021) (overruling plaintiff's objection to exclusion of unvaccinated potential jurors).

18.5.4 *Kinder Morgan Prod. Co., LLC v. Scurry County Appraisal Dist.*, No. 11-20-00258 (Tex. Ct. App. Dec. 30, 2021) (granting new trial after failure of remote protocol and technical difficulties with attorney participation in remote voir dire).

18.5.5 *Nuvasive, Inc. v. Absolute Medi., LLC*, Case No. 6:17-cv-2206-CEM-GJK (M.D. Fla. Jan. 10, 2022) (vacating arbitration award and issuing show cause order in response to text messaging

between one party's corporate president and a witness during latter's remote testimony).

18.5.6 *Pain Relief Centers, P.A.*, et al., Cases 10–CA–260563, et al., fn. 2 (National Labor Relations Board, Feb. 23, 2022) ("[T] the courtroom deputy's role is purely administrative: ensuring that the hearing runs smoothly, allowing the judge to focus on the witness testifying, and mitigating technological glitches. As the judge advised the parties at the outset of the hearing, the courtroom deputy is 'not here in an attorney rol[e] but rather, as a Courtroom Deputy to assist me and to assist you, if necessary, with technical Zoom-related issues. She has a lot of experience with Zoom and she won't be answering any of your legal-related questions or rule on any issues; that's for me. But she is here to help us manage transfer of documents and just help us as needed with Zoom issues.'")

18.5.7 *Carroll v. Trump*, 20-cv-7311 (LAK), 2024 U.S. Dist. LEXIS 4453 (S.D.N.Y. Jan. 9, 2024) (addressing, among other trial-related disputes, admissibility of "Access Hollywood" video recording of defendant's statements and denying his request to exclude it on Fed. R. Evid. 403 grounds)

18.5.8 *Elliott v. Cartagena*, 84 F.4th 481 (2d Cir. 2023) (concluding the district court had erred in denying plaintiff's request to conduct discovery prior to entry of summary judgement and in finding that draft agreement between the parties was

admissible as a duplicate original under Fed. R. Evid. 1003)

18.5.9 *Hart v. State*, 688 S.W.3d 883 (Tex. Ct. Crim. App. May 8, 2024) (reversing judgement below and holding that trial court had abused its discretion by admitting rap videos to show defendant's character and sophistication; "probative value of the rap videos and lyrics was outweighed by the overwhelming potential for prejudice and confusing the issues").

18.5.10 *State v. Puloka*, No. 21-1-04851-2 KNT (Wash. Super. Ct. Mar. 29, 2024) (rejecting admissibility of AI-enhanced evidence under Frye v. United States test).

18.5.11 *United States v. Jordan*, 20-CR-305 (LDH), 2024 WL 343970 (E.D.N.Y. Jan. 30, 2024) (denying Government's motion to admit rap videos and interview videos portraying defendant and his music given absence of nexus to alleged criminal conduct)

18.5.12 *Kohls v. Ellison*, Court File No. 24-cv-03754 (D. Minn.) (Order Granting in Part and Denying in Part Plaintiffs' Motion to Exclude Expert Testimony and Denying Defendants' Motion for Leave to File an Amended Expert Declaration, filed Jan. 10, 2025); (Order Denying Plaintiffs' Motion for a Preliminary Injunction, filed Jan. 10, 2025).

18.5.13 *Matter of Weber*, 2024 NY Slip Op 24258 (Surrogate's Court, Saratoga County Oct. 10, 2024).

18.6 Further Reading

18.6.1 P.M. Kessimian & K.J. O'Donnell, *Five Tips for Admitting Electronically Stored Information into Evidence*, PRACTICE POINTS (ABA: July 14, 2023).

18.6.2 E. Lasker, et al., *Expert Evidence Rule Will Be a Tool to Improve Scientific Testimony*, BLOOMBERG LAW (Nov. 27, 2023).

18.6.3 A.S. Persky, *Moons, Fire and Pigs: Emojis Can Be Confusing in Court*, ABA JOURNAL (July 2, 2024).

18.6.4 G. Rossi, *Four Rules to Establish that Your Evidence is Legit*, LITIGATION, Vol. 49, No 4, p. 52 (ABA: Summer 2023).

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

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

19. Sanctions

19.1 Sanctions may be imposed for a broad range of discovery misconduct, including, but not limited to, the loss of ESI. Discovery misconduct may therefore be sanctionable under multiple rules or statutes or under the court's inherent authority. These include Rules 26(g)(1) and 37(b) and their state equivalents.

19.1.1 Judges should evaluate any discovery misconduct and determine which rule or rules apply to that misconduct as well as the standard for the imposition of sanctions under the selected rule.

19.1.2 The risk of sanctions is a serious concern in eDiscovery, and consideration of sanctions is a sensitive and time-consuming task that a judge might be required to undertake. Moreover, as with discovery disputes generally, motions for sanctions run the risk of extended—and expensive—satellite proceedings.

19.1.3 The 2015 amendment to Federal Rule of Civil Procedure 37(e) has altered the landscape of sanctions under the Federal Rules. Several states have followed suit. The *Resources* will not delve into that amendment in detail but will highlight significant features of Rule 37(e). These features are:

- Rule 37(e) applies only to the loss of ESI.
- Rule 37(e) is applicable only after a duty to preserve had arisen.
- Rule 37(e) is premised on the failure of a party to have taken "reasonable steps" to avoid the loss of relevant ESI.
- If ESI is lost as the result of negligent conduct and the opposing party has been prejudiced by the loss of that ESI, the court can order "measures no

greater than necessary to cure the prejudice."

- If a party "acted with the intent to deprive another party of the information's use in the litigation," the court may impose case-terminating or analogous sanctions, including a mandatory adverse inference charge.

19.1.5 Most states do not have an equivalent to Rule 37(e) and sanctions are governed by more general sanctions rules or the common law of spoliation.

19.2 Issues presented

19.2.2 Sanctions motions may present questions about the process used by a party to respond to an adversary's discovery requests. Resolution of such questions may require "discovery about discovery," that is, determining what process was used and what the results of that process did or did not include. Any such resolution is seldom relevant to the merits of the action before the judge but may be necessary to resolve the dispute. This discovery about discovery should be narrowly tailored, and the importance of proportionality stressed.

19.2.3 "Piecemeal" motion practice can lead to excessive cost, delay, and stress on already-strained court resources. The timing of a sanctions motion can be troublesome for a judge. A sanctions motion can disrupt other discovery and other

case management. Therefore, assuming that a judge has discretion to do so, the motion might be scheduled to be made only after all discovery has been completed.

19.3 Suggested judicial management strategies

19.3.1 Inquire, whenever the word "sanction" arises, about the nature of the dispute. Ascertain *exactly* what relief is sought and why.

19.3.2 Conduct an informal proceeding in the first instance. Determine whether a party, rather than seeking a sanction, is in fact requesting an extension of some deadline.

19.3.3 In lieu of allowing a formal motion, consider whether other discovery may be conducted that could eliminate, or at least reduce, the need for the motion.

19.3.4 Consider whether to postpone any ruling on the imposition of sanctions or the amount of sanctions upon completion of discovery or following the resolution of the action on its merits.

19.4 Representative Decisions

19.4.1 *GN Netcom, Inc. v. Plantronics*, 930 F.3d 76 (3d Cir. 2019) (deletion of relevant email by executive of defendant led to monetary sanctions and adverse inference instruction; jury verdict in defendant's favor vacated and remanded for new trial, and trial court directed to allow expert testimony related to effect of spoliation).

19.4.2 *Bellamy v. Wal-Mart*, No. SA-18-CV-60-XR, 2019 WL 3936992 (W.D. Tex. Aug. 19, 2019) (sanctions imposed for failing to preserve surveillance video taken from camera positioned to view accident, while preserving video from another camera positioned elsewhere).

19.4.3 *Guarisco v. Boh Bros. Constr. Co.*, LLV, 421 F. Supp. 3d 367, 381 (E.D. La. Oct. 3, 2019) (sanctions imposed under inherent power for alteration of photographs although photographs not "lost" under Rule 37(e); "it would be premature . . . to find that Rule 37(e) applies here, as there is no proof any of the [other] digital evidence at issue is permanently lost.").

19.4.4 *Mannion v. Ameri-Can Freight Sys. Inc.*, No. CV-17-03262-PHX-DWL, 2020 WL 417492 (D. Ariz. Jan. 27, 2020) (court rejected proposed spoliation instruction and held that nonproduction or spoliation was to be resolved by the judge, not the jury).

19.4.5 *Carroll v. Trump*, 20-cv-7311 (LAK) (S.D.N.Y. Feb. 7, 2024) (addressing, among other things, duty to preserve, meaning of prejudice, and intent to deny use of ESI to other party under Rule 37(e) and concluding that no relief warranted for plaintiff's loss of email given the she was subject to cross-examination on loss, defense counsel presented summation that referenced loss, and jury instructed on its use of the loss)

19.4.6 *Freeman v. Giuliani*, Civil Action No. 21-3354 (BAH) (D.D.C. Aug. 30, 2023 (among other things, entering default judgment as to liability on defendant for his failure to preserve ESI)

19.4.7 *Goldstein v. Denner*, C.A. No. 2020-1061-JTL (Del. Ch. Jan. 24, 2024) (imposing sanctions for defendants' loss of text messages that include imposition of presumptions against them at trial and imposing heightened burden of proof to rebut presumptions)

19.4.8 *United States v. Google LLC*, Case No. 20-cv-2010 (APM) (D.D.C. Aug. 5, 2024) (declining to impose Rule 37(e) sanctions on defendant for its failure to preserve chat evidence because doing so would not "move the needle on the Court's assessment" of defendant's liability under Section 2 of Sherman Act).

19.5 Further reading

19.5.1 Rule 37(g)(1)(C)(ii), Rules of Civil Procedure for the Superior Courts of Arizona (setting out "factors that a court should consider in determining whether a party took reasonable steps to preserve" ESI).

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

20. Post-judgment costs

20.1 This stage of litigation looks to the award of costs after a party secures a final judgment in its favor. It does not address cost sharing or shifting during discovery.

20.1.1 Under the Federal Rules, a prevailing party "should be allowed" its costs. In the first instance, costs are taxed by the clerk of the district court in which a judgment is entered.[30] Awardable costs are defined in 28 U.S.C. §1920 and include costs associated with "[f]ees for . . . electronically reported transcripts necessarily obtained for use in the case,"[31] and "[f]ees for exemplification and the costs of making copies of any materials where the copies are necessarily obtained for use in the case."[32] Federal courts are divided regarding what e-discovery charges are recoverable under Section 1920(4). We are unaware of any state decisions that have addressed post-judgment awards of ESI-related costs.

20.2 Issues presented

20.2.1 Understanding what vendor services were specifically provided is crucial to understanding whether section 1920 will allow for the recovery of those expenses. Require the requesting party to provide details as to what services were

30. FED. R. CIV. P. 54(d)1.

31. 28 U.S.C.A. § 1920(2) (2008).

32. 28 U.S.C.A. § 1920(4) (2008).

performed and how the expenses were necessarily obtained for use in the case.

20.2.2 Assuming that ESI-related costs *may* be taxed under a statute or rule, what challenges can be raised to the application by a losing party? For example, the necessity and reasonableness of the cost of creation of a database cannot be calculated with a simple mathematical formula and may require expert opinion. The court should consider whether a clerk can take expert opinion into consideration when taxing costs.

20.2.3 The reasonable expenses associated with the conduct of remote or hybrid proceedings may be recoverable as costs. Conversely, the refusal to engage in remote or hybrid proceedings, without good cause, may be a consideration in reducing or reallocating the cost recovery.

20.3 Suggested judicial management strategies

20.3.1 Direct the parties to confer at the Rule 26(f) conference or its state equivalents or prior to the first case management conference and to agree on what ESI-related costs might be taxable under the controlling statute or rule. This might also inform the court on proportionality.

20.4 Representative decisions and orders

20.4.1 *United States ex rel. Barko v. Halliburton Co.*, 954 F.3d 307 (D.C. Cir. Mar. 27, 2020) (adopting "narrow" interpretation of taxable eDiscovery-

related costs under §§ 1920(2) and (4)) (the only e-discovery costs that KBR may recover are those incurred in step (4)—converting electronic files to the production formats (in this case, PDF and TIFF) and transferring those production files to portable media (here, USB drives). These tasks resemble the final stage of "doc review" in the pre-digital age: photocopying the stack of responsive and privilege-screened documents to hand over to opposing counsel.).

20.4.2 *Consumer Fin. Prot. Bureau v. Weltman, Weinberg & Reis Co., L.P.A.*, 342 F. Supp. 3d 766 (N.D. Ohio Oct. 22, 2018) (court allowed as costs expenses for loading and exporting data into an e-Discovery vendor platform as "copying." The opinion further stated that "data conversion, audio transcription, and export of data, all suggest a replication of data that would fit the broader definition of electronic "copying.").

20.4.3 *Gonzales v. Pan Am. Labs., L.L.C.*, No. 3:14-CV-2787-L, 2018 WL 2321896, at *5 (N.D. Tex. May 4, 2018), *report and recommendation adopted*, No. 3:14-CV-2787-L, 2018 WL 2317749 (N.D. Tex. May 22, 2018) (court rejected costs associated with gathering and hosting data in a platform because "the United States Supreme Court has underscored the 'narrow scope of taxable costs' and has emphasized that 'taxable costs are limited to relatively minor, incidental expenses as is evident from §1920.'" (*citing Taniguchi v. Kan Pacific Saipan, Ltd.*, 566 U.S. 560, 573 (2012)). *But see*

Javeler Marine Servs. LLC v. Cross, 175 F. Supp. 3d 756 (S.D. Tex. 2016) (creation of forensic electronic images of defendants' hard drives qualified as "making copies of any materials," as required for expense of creating images to be taxable as cost to employer; forensic electronic images were necessarily obtained for use in the case; but defendants were not entitled to reimbursement for expense of keyword searches.)

20.4.4 *Vital v. Varco*, No. CV H-12-1357, 2015 WL 7740417, at *5 (S.D. Tex. Nov. 30, 2015), *aff'd sub nom. Vital v. Nat'l Oilwell Varco, L.P.*, 685 F. App'x 355 (5th Cir. 2017) (court declined to award as costs monthly expenses associated with maintaining a database of electronically stored information used to locate, retrieve, and store the plaintiffs' emails.)

20.4.5 Parker Hannifin Corp. v. Fed. Ins. Co., 23 F. Supp. 3d 588 (W.D. Pa. 2014) (court allows parties to expand the scope of discovery, on the condition that any additional ESI collection costs will be considered "as a fee for exemplification or a cost of making copies," recoverable by the prevailing party under 28 U.S.C. §1920(4).)

20.4.5 *Eolas Techs. Inc. v. Adobe Sys.*, Inc., 891 F. Supp. 2d 803 (E.D. Tex. 2012), *aff'd sub nom. Eolas Techs. Inc. v. Amazon.com, Inc.*, 521 F. App'x 928 (Fed. Cir. 2013) (district court considered whether §1920(4) reached several types of costs that may be generally classified as electronic discovery costs: (1) document scanning, (2) document

collection, (3) document processing, (4) document hosting, and (5) conversion to TIFF format. The court concluded that "[d]ocument scanning is essentially copying paper documents to electronic form" and would be a recoverable cost. The court found that costs for document collection, processing, and hosting were not recoverable costs because §1920(4) "is not so broad as to cover general electronic discovery costs that precede copying or scanning of materials." The court also held that conversion to TIFF, as opposed to production in native format, was not necessary, and thus not a taxable cost.)

20.4.6 *Chenault v. Dorel Indus., Inc.*, No. A-08-CA-354-SS, 2010 WL 3064007, at *1 (W.D. Tex. Aug. 2, 2010) (prevailing defendant created an electronic database to respond to the plaintiff's discovery requests. The court noted that the electronic production saved the cost of printing and copying 800,000 pages, at an estimated cost of $120,000. Because the electronic data "was produced in lieu of extremely costly paper production" and the defendant was "seeking to save costs by not printing out thousands of pages of documents which would have otherwise been required in response" to discovery requests, the court found that the expense fell within the category of costs recoverable for fees and disbursements for printing.)

If you would like to contribute anything else that illustrates the strategies above, please contact us at resources@sedonaconference.org.

V. ADDENDUM

This addendum is not about case management. Rather, it is about use of artificial intelligence ("AI") and generative artificial intelligence ("GenAI") by judges in the discharge of their duties. It is not intended to be exhaustive, and indeed the landscape in this area changes almost daily.

Opinions addressing use of AI or GenAI in decision making:

- *Ross v. United States*, , 331A. 3d 220 (D.C. Ct. App. Feb. 20, 2025) (majority, concurring, and dissenting opinions all discuss use of Chat GPT)
- *Snell v. United Specialty Ins. Co.*, 102 F.4th 1208, 1221-35 (11th Cir. 2024) (Newsom, J. concurring)

Policies about AI or GenAI use:

- H.B. Dixon Jr., *et al., Navigating AI in the Judiciary: New Guidelines for Judges and Their Chambers*, 26 SEDONA CONF. J. 1 *(forthcoming 2025)*.
- BJA AI Statement of Principles (Washington Courts Board for Judicial Administration: Feb. 21, 2025).
- Statement of Principles for the New Jersey Judiciary's Ongoing Use of Artificial Intelligence, Including Generative Artificial Intelligence(as approved by NJ Sup. Ct Jan. 23, 2024).
- California Courts AI Task Force, Model Policy for Use of Generative Artificial Intelligence, presented to Judicial Council of California Feb. 21, 2025.

MOVING THE LAW FORWARD IN A REASONED & JUST WAY